10ème Rapport d'activités 2002/2003

Préposé fédéral à la protection des données

Rapport d'activités 2002/2003 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 2002 au 31 mars 2003.

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

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Le 11 septembre 2001 a été l'objet principal de mon avant-propos l'an dernier. Mes préoccupations portaient sur la manière dont un Etat de droit démocratique pouvait faire face à ce défi sans remettre en cause ses propres fondements.

Où en sommes-nous une année plus tard? L'espoir que le monde réagira avec la circonspection voulue aux nouvelles menaces ne s'est malheureusement pas encore confirmé. Dans le cadre national, du point de vue de la protection de la personnalité, il est vrai qu'aucune réaction démesurée n'est apparue à ce jour. La pression vient de l'extérieur: dans le combat contre «l'axe du mal», l'administration Bush recherche l'hégémonie dans tous les domaines. De plus en plus, des législations nationales sont foulées par les Etats-Unis qui tentent de soumettre le reste du monde à son système juridique. Un exemple récent: les Etats-Unis exigent de toutes les compagnies aériennes dès le 5 mars 2003 la remise des données personnelles de leurs passagers, de leur religion et préférences alimentaires au numéro de carte de crédit. Ceci est critiquable non seulement en raison de la sensibilité des données exigées, mais surtout par la manière dont ce besoin de données est imposé internationalement. Dans une loi, les autorités américaines exigent des compagnies aériennes que les données de tous les passagers arrivants aux Etats-Unis leur soient communiquées à l'avance. Les contrevenants sont menacés de peines allant jusqu'au retrait des autorisations d'atterrissage. Aucun accord n'a encore été conclu à ce sujet avec les autorités suisses. En absence d'accord, la compagnie aérienne Swiss se verrait finalement contrainte de transmettre des données, même en violation du droit national. En effet, notre législation impose qu'une transmission de données à un autre pays n'est autorisée que si le pays concerné dispose d'une protection des données comparable. Ceci n'est justement pas le cas aux Etats-Unis, raison pour laquelle cette communication de données ne serait autorisée aux termes de notre droit que si en même temps était conclue entre les Etats-Unis et la Suisse une convention qui fixe pour ces données des conditions de protection comparables à celles de notre législation.

La manière de procéder américaine ainsi décrite n'est pas un cas isolé. De plus en plus, nous allons être confrontés au fait que, sous le couvert d'une lutte antiterroriste, les Etats-Unis veulent tenter de saper la souveraineté en matière législative des pays sans négociations, par un diktat unilatéral.

Le fait que cette tentative d'influence doit absolument être prise au sérieux et qu'elle constitue une mise en danger grave de notre ordre juridique est évident si l'on considère la manière dont l'administration Bush combat le terrorisme dans son propre pays: les Etats-Unis, avec le «Patriot Act», ont depuis longtemps choisi la voie d'un

ordre répressif qui ne fait plus grand cas de la protection de la personnalité. Cette loi a été introduite juste après le 11 septembre 2001 pour déceler à temps des activités terroristes. Entre autres, la loi va jusqu'à permettre aux autorités de surveiller des usagers de bibliothèques, même en l'absence de tout indice d'agissements criminels. Ceci permet ainsi aux collaborateurs du FBI, sans en informer la personne concernée, de réclamer toutes les pièces telles que livres, documents, journaux ou disques durs d'ordinateurs. Les surveillances téléphoniques et Internet sont simplifiées. Le FBI peut mettre des personnes sous écoute même sans présomption. Le gouvernement Bush veut durcir encore cette loi afin de pouvoir détenir secrètement même des citoyens américains. Avec le «Total Information Awareness», le Pentagone veut en outre consigner dans une banque de données des informations médicales, financières, fiscales, parmi bien d'autres. Les défenseurs des droits des citoyens américains mettent en garde contre une dangereuse évolution aux Etats-Unis. Le directeur de l'organisation américaine de défense des libertés individuelles ACLU, Barry Steinhardt, disait récemment dans une interview: «Une combinaison d'innovations techniques ultrarapides et de l'érosion de la protection de la sphère privée menace de transformer Big Brother, un danger souvent cité, mais bien éloigné, en une partie intégrante du quotidien américain.» Le rapport publié par cette organisation en janvier 2003 porte le titre: «Un monstre plus gros, des chaînes plus faibles: la croissance d'une société américaine de la surveillance.» Des mesures qui servent à la lutte contre le terrorisme doivent bien entendu être soutenues par la Suisse aussi. Il faut par contre dresser des barrières, car le point est entre-temps atteint où la lutte contre le terrorisme non seulement entre en collision avec la protection des données, mais commence à devenir une menace pour notre Etat de droit. Il est à craindre que les Etats-Unis n'imposent cette mentalité de surveillance chez nous aussi, avec des pressions directes ou indirectes.

Eu égard à ces faits, nous devons, l'année du 10ème anniversaire de notre loi sur la protection des données, tirer une conclusion désillusionnée: certes, dans le cadre national, grâce à cette loi, la sensibilité et la conscience des potentiels de menaces de l'évolution technique sur les droits de la personnalité des citoyens ont bien augmenté de façon réjouissante. Mais à quoi bon, si en fin de compte ces acquis sont furtivement abrogés par une puissance mondiale aspirant à l'hégémonie et qui, en ce qui concerne la protection des données et de la personnalité, se trouve au niveau d'un pays en voie de développement?

Ce constat ne doit cependant pas conduire à croire que nous n'aurions plus à résoudre de problèmes internes relevant de la protection des données et que les évolutions menaçant la personnalité ne trouveraient leur origine qu'à l'étranger. Ceci nous bercerait effectivement d'un faux sentiment de sécurité. Indépendamment de la pression américaine, le penchant croissant à installer une caméra vidéo dans les moindres

recoins dans l'espoir d'obtenir plus de sécurité sévit chez nous aussi. Même s'il n'est pas contestable que dans certaines circonstances cette technique peut parfaitement rendre d'utiles services, il faut pourtant constater qu'elle est souvent superflue, inadéquate et disproportionnée, et va parfois jusqu'à faire miroiter une fausse sécurité. Ainsi, un parking ne devient pas plus sûr pour les femmes parce que des caméras y sont installées. Il est facile de se soustraire à l'identification en se couvrant le visage. L'endroit ne deviendra plus sûr que s'il est surveillé et contrôlé par des personnes. Location based services (emploi du téléphone mobile par des entreprises de marketing à des fins publicitaires) et pervasive computing (petits émetteurs, souvent invisibles, pouvant être installés partout, jusque dans les vêtements et les denrées alimentaires, pour fournir des données) sont des phénomènes qui intéressent en premier lieu nos publicitaires et spécialistes du marketing, mais dont le potentiel d'atteinte à la personnalité est immense. Ou, comme le formulait en début d'année Marie-Theres Tinnenfeld, professeur allemande de droit: «Il est à craindre aujourd'hui qu'une surveillance étatique sans mesure et une chasse aux données sans limites des milieux économiques ne puissent détruire la sphère privée.»

Hanspeter Thür

Répertoire des abréviations

AGX	Groupe de travail Santé
AI	Assurance-invalidité
APG	Allocations pour perte de gain
ASA	Association Suisse d'Assurances
AVS	Assurance vieillesse et survivants
BDNS	Banque de données nationale pour le sport
CHOP	Classification Suisse des interventions chirurgicales
CIRCA	Communication & Information Resource Centre Administrator
CP	Code pénal suisse
DFI	Département fédéral de l'intérieur
FMH	Fédération des médecins suisses (Foederatio Medicorum Helveticorum)
ICD-10	International Classification of Diseases, 10th revision
IDA	Interexange of Data between Administrations (Echange d'informations entre administrations publiques)
LAA	Loi fédérale sur l'assurance-accidents
LAGH	Loi fédérale sur l'analyse génétique humaine
LAMal	Loi fédérale sur l'assurance-maladie
LCC	Loi fédérale sur le crédit à la consommation
OBDNS	Ordonnance sur la banque de données nationale pour le sport
OFAS	Office fédéral des assurances sociales
OFJ	Office fédéral de la justice
OFS	Office fédéral de la statistique
OFSPO	Office fédéral du sport
RAI/RUG	Resident Assessment Instrument / Ressource Utilization Groupes
Tarmed	Tarif médical (Le tarif de la Médecine suisse)

1. Droits fondamentaux

1.1 Modernisation de la protection des données

Suite à deux motions parlementaires, le Conseil fédéral a adressé un message aux Chambres fédérales proposant une révision partielle de la loi fédérale du 19 juin 1992 sur la protection des données (LPD) et la ratification du protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Le projet de loi sur la transparence, également transmis au Parlement, entraînera aussi une modification de la LPD. Enfin selon l'avancement des négociations bilatérales entre la Suisse et l'Union européenne, une révision plus substantielle de la LPD pourrait rapidement s'avérer nécessaire. Le PFPD est dans l'ensemble d'accord avec les modifications proposées. Il regrette néanmoins que la révision ne soit pas plus ambitieuse.

Révision de la loi fédérale sur la protection des données

Donnant suite 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 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 transmis aux Chambres fédérales le 19 février 2003, un 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)

Le projet de révision renforce la position des personnes concernées, en particulier du fait de l'introduction d'une obligation de transparence lors de la collecte de données personnelles. Toute collecte de données devra ainsi à l'avenir être reconnaissable pour la personne concernée. Celle-ci devra au minimum connaître les finalités du traitement. Lors de la collecte de données sensibles ou de profils de la personnalité, le responsable du traitement devra informer activement les personnes concernées au moins de l'identité du maître du fichier, des finalités du traitement pour lequel les données sont collectées et des catégories de destinataire des données si la communication est envisagée. Tout comme pour le droit d'accès, l'information de la personne concernée peut être restreinte dans certaines conditions. Les personnes concernées devront également être expressément informées lorsqu'une décision produi-

sant des effets juridiques à leur égard ou les affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à estimer certains aspects de leur personnalité. Dans le secteur privé, le droit de s'opposer à un traitement sera rendu plus effectif, notamment en incitant le responsable du traitement à se déterminer lors d'une requête d'une personne concernée.

Le régime des flux transfrontières de données sera revu. La déclaration préalable sera abandonnée. L'interdiction de transfert lorsque la personnalité des personnes concernées se trouve gravement menacée est maintenue. Le projet introduit cependant des dérogations, notamment lorsque des garanties appropriées (recours à des clauses contractuelles de protection des données, règlement de protection des données pour les groupements d'entreprises) sont fournies par le responsable de traitement. Ces garanties devront être annoncées au PFPD qui pourra le cas échéant intervenir. L'annonce des fichiers est maintenue tant pour les organes fédéraux que pour les personnes privées. Toutefois, des dérogations à l'annonce seront introduites dans la loi et la procédure d'annonce sera simplifiée, notamment par l'introduction, dans un avenir proche, de la possibilité pour le maître de fichier de déclarer ses fichiers en ligne. Le registre des fichiers sera publié sur Internet, ce qui facilitera sa consultation. Le projet innove en introduisant, sous forme de norme incitative, le recours à la certification des produits et des systèmes de traitement des données personnelles (audit, label de qualité de protection des données). Le PFPD pourra, dans le cadre de ses compétences, s'assurer que les entreprises certifiées respectent les exigences de protection des données et que les entreprises qui procèdent à la certification et à la «labelisation» agissent conformément aux exigences de la protection des données. Il pourra fixer le cadre des évaluations et émettre le cas échéant des recommandations.

En outre, le projet précise la réglementation relative au traitement des données sur mandat, notamment lorsque des organes fédéraux font traiter des données par des tiers. Dans ce cas, les organes fédéraux pourront effectuer des contrôles auprès de ces tiers. En réponse à la motion «liaisons on-line», le Conseil fédéral pourra autoriser, pour une durée limitée, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre de projets «pilotes», avant que la base légale formelle y relative ne soit entrée en vigueur. Le projet de révision fixe également les exigences minimales auxquelles la législation cantonale doit répondre lorsqu'un canton traite des données en exécution du droit fédéral. Enfin, le PFPD pourra recourir auprès de la Commission fédérale de la protection des données contre une décision d'un département ou de la Chancellerie fédérale qui ne donne pas suite à une recommandation adressée à un organe fédéral qui l'a refusée ou qui ne l'a pas suivie. Dans le secteur privé, le PFPD voit son pouvoir d'intervention renforcé. Il pourra en effet à l'avenir enquêter sur des traitements de données sensibles ou de profils de la personnalité,

ainsi que sur des communications régulières de données indépendamment du fait que les fichiers concernés par ces traitements font l'objet d'une annonce en vue de leur enregistrement dans le registre des fichiers.

Protocole additionnel à la Convention 108

Le premier protocole additionnel à la Convention 108 a été adopté par le Comité des Ministres du Conseil de l'Europe, le 23 mai 2001 et ouvert à la signature des Etats, le 8 novembre 2001. A ce jour, trois Etats parties à la Convention 108 ont ratifié le protocole additionnel et 18 autres l'ont signé. Suite aux résultats positifs de la procédure de consultation, la Suisse a signé le protocole le 17 octobre 2002. L'objectif poursuivi par ce protocole est de renforcer la mise en œuvre des principes contenus dans la Convention 108 et en particulier de tenir compte de l'augmentation croissante des flux transfrontières de données, notamment vers des destinataires établis dans un Etat non contractant. Le protocole règle tout d'abord l'obligation des Etats contractants de se doter d'une ou de plusieurs autorités chargées de veiller au respect des dispositions nationales de protection de données. Ces autorités doivent agir de manière indépendante et bénéficiées de compétences effectives, notamment d'investigation et d'intervention. Elles sont une partie intégrante du système de contrôle de la protection des données dans une société démocratique. Du fait de la dimension internationale des transferts de données personnelles et afin d'améliorer l'harmonisation des solutions de protection des données, les autorités de contrôle des Etats contractants sont appelées à coopérer entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant des informations.

Le protocole règle ensuite les flux transfrontières de données vers des pays tiers. Ainsi, le transfert de données personnelles vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention 108 ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré. Le protocole aménage cependant des dérogations à l'exigence du niveau de protection adéquat. Le transfert peut ainsi être autorisé si le droit interne de l'Etat contractant d'où les données sont communiquées, le prévoit pour des intérêts spécifiques de la personne concernée ou pour des intérêts légitimes prévalant les intérêts de la personne concernée. Le transfert est également possible si des garanties résultant notamment de clauses contractuelles sont prises par le responsable du transfert. Ces garanties doivent inclure les éléments pertinents de la protection des données et préserver les droits des personnes concernées. Elles doivent avoir été jugées suffisantes par les autorités de protection des données compétentes.

Le projet de révision de la LPD permet de mettre la législation fédérale en conformité avec les exigences du protocole additionnel et à la Suisse de le ratifier. La ratification du protocole est importante pour la Suisse notamment du fait des nombreux échanges d'informations avec les pays membres de l'Union européenne. Le respect des exigences de la Convention 108 et de son protocole additionnel constituera à l'avenir un élément déterminant dans l'appréciation du niveau adéquat de protection des Etats tiers. Les cantons devront également adapter leur législation et pour certains renforcer les compétences et l'indépendance de leurs autorités de contrôle.

Négociations bilatérales II entre la Suisse et l'Union européenne

La Suisse et l'Union européenne ont entamé de nouvelles négociations bilatérales. Ces négociations ont trait en particulier aux services, à la fiscalité de l'épargne, aux accords de Schengen et à la Convention de Dublin sur l'asile. Si ces négociations aboutissent à un accord, la Suisse devra reprendre une partie de l'acquis européen. Parmi cet acquis figure la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. La reprise de cet acquis implique une révision plus conséquente de la LPD que celle présentée par le Conseil fédéral. Les principales différences avec le droit européen concernent en particulier les définitions et la terminologie utilisée, le champ d'application de la directive qui est plus large que celui de la LPD, le régime des données sensibles qui, dans le secteur privé, est plus sévère en droit européen, l'information explicite des personnes concernées lors de la collecte des données, qui couvre toutes les données personnelles indépendamment de leur nature, le droit de ne pas être soumis à une décision individuelle automatisée, absent de notre législation et le droit d'accès qui est plus large dans la directive européenne. Le régime de la notification des traitements en droit européen diffère également du droit suisse, notamment quant aux informations à fournir, à l'étendue de la notification et à l'examen préalable des traitements à risque. Enfin, les compétences et les pouvoirs des autorités de contrôle de la protection des données paraissent plus étendues dans la directive européenne. Plusieurs législations des Etats membres de l'Union européenne attribuent des pouvoirs de décision et de sanctions à leurs autorités de protection des données. Les cantons devront également revoir leur législation. La question se pose de savoir si la Confédération ne devait pas disposer d'une compétence permettant une application de la LPD, du moins à titre supplétif, à l'ensemble des traitements de données effectués par des organes cantonaux ou communaux en l'absence d'un niveau de protection des données adéquat.

La transposition de la directive européenne ne serait pas désavantageuse pour la Suisse. Même si dans un premier temps, on peut éventuellement s'attendre à des réactions négatives de l'économie privée, les entreprises suisses actives en Europe trouveraient également des avantages substantiels à une harmonisation plus complète de notre droit avec le droit européen. Cette transposition permettra d'éviter des obstacles à la circulation des données avec les Etats européens et offrira aux personnes concernées un niveau de protection équivalent et des droits identiques à ceux des ressortissants de l'Union européenne. Elle assurera une plus grande homogénéité des pratiques et de la jurisprudence et une participation au développement du droit européen. Elle devrait nous permettre également de participer aux travaux du groupe de travail mis en place par la directive européenne.

Projet de loi sur la transparence de l'administration

Le Conseil fédéral a également adopté le 12 février 2003 un message relatif à la loi fédérale sur la transparence (LTrans; FF 2003 1807) et l'a transmis aux Chambres fédérales. Ce projet de loi vise à garantir l'accès du public aux documents officiels et à promouvoir la transparence de l'administration. L'accès aux documents officiels porte également sur des données personnelles. En règle générale, ces documents seront anonymisés avant d'être transmis aux personnes qui les requièrent. Toutefois, l'anonymisation n'est pas toujours possible et dans certaines situations, l'administration pourrait être amenée à transmettre des données personnelles à des tiers. Dans ces cas, la LPD sera applicable et en particulier la licéité de l'accès sera régie par les dispositions régissant la communication de données personnelles. La personne concernée pourra demander à être consultée préalablement à la communication des données requises. Elle devra être consultée si la demande porte sur des données sensibles ou des profils de la personnalité. Le projet de loi institue un médiateur en cas de conflit entre l'administration et l'administré au sujet d'une demande d'accès. La médiation sera assurée par le PFPD qui se voit ainsi attribuer de nouvelles tâches. Ce système correspond à la position prise par le PFPD lors de la procédure de consultation (voir 7ème rapport d'activités, chapitre II.7). La LTrans prévoit également une modification de la LPD permettant de communiquer des données personnelles qui sont rendues accessibles dans le cadre de l'information du public effectuée d'office par les autorités ou en vertu de la LTrans pour autant que les données soient en rapport avec l'accomplissement de tâches publiques et qu'il existe un intérêt prépondérant à communiquer ces données. En outre, ces données pourront également être publiées sur Internet. La diffusion sur Internet sera également envisageable lorsqu'une base légale prévoit la publication des données. Toutefois, le recours à Internet ne doit pas être automatique du fait de la publication ou de l'accessibilité des don-

nées à tout un chacun. Le principe de proportionnalité devra être respecté. En outre, les données devront être effacées une fois que le but d'intérêt public ayant justifié la publication aura été atteint, notamment pour assurer le droit à l'oubli. Dans certains cas, il conviendra de limiter l'accès aux données, notamment en restreignant les mécanismes de recherche des données.

Position du PFPD concernant la révision de la LPD

Le PFPD soutient dans l'ensemble les propositions de modification de la LPD figurant dans les deux messages susmentionnés. Comme nous l'avions déjà relevé dans notre 8ème rapport d'activités (chapitre I.12), nous aurions souhaité une révision plus étendue de la LPD et notamment un rapprochement plus conséquent avec le droit européen. En particulier, nous saluons l'introduction de la certification et du label de qualité de protection des données qui contribuent à renforcer l'autonomie et la responsabilité des maîtres de fichier. Nous relevons également l'équilibre qui a été trouvé dans la LTrans entre l'accès aux documents officiels et les exigences de la vie privée. Par contre, nous avons des réserves quant à l'introduction d'une disposition permettant au Conseil fédéral d'autoriser, avant l'entrée en vigueur d'une loi au sens formel, le traitement automatisé de données sensibles ou de profils de la personnalité. Nous estimons tout d'abord que cette disposition va au-delà de la motion «liaisons on-line» qui demande une base légale uniquement pour les accès en ligne. Ensuite, tout en reconnaissant la nécessité d'aménager le principe de légalité, notamment pour tenir compte de la complexité des systèmes de traitement de données personnelles et de l'évolution dans l'accomplissement des tâches des organes fédéraux, nous aurions souhaité une réflexion plus approfondie sur les exigences du principe de légalité et les modalités de sa mise en œuvre. En particulier à l'instar de certaines législations européennes, certains traitements pourraient être soumis à l'autorisation préalable du Préposé fédéral à la protection des données. Dans une étape ultérieure, nous estimons nécessaire de renforcer les droits de la personne concernée et notamment d'alléger la procédure dans le secteur privé pour permettre aux individus de faire valoir leurs droits, ainsi que d'encourager le recours aux technologies de la vie privée, en imposant par exemple aux responsables de traitement l'obligation de développer des outils permettant aux individus d'exercer leurs droits lorsqu'ils recourent à des services en ligne. L'autoréglementation pourrait également être développée. Toutefois, une plus grande autonomie des responsables de traitement doit avoir pour conséquence la mise en place de moyens de contrôle préventifs et répressifs en cas d'abus. Cela implique qu'à l'avenir, le PFPD ait un rôle plus proactif. L'objectif ainsi poursuivi est d'éviter que les individus se trouvent dépourvus de toute protection lorsque des données les concernant font l'objet d'un traitement. Il est dès lors néces-

saire de développer une politique qui promeut la reconnaissance et le respect des principes de la protection des données et qui permet aux personnes concernées d'exercer effectivement leurs droits. Le PFPD doit ainsi veiller à ce que ces règles soient respectées et intégrées dans les processus de traitements des données. Cette approche nécessite de revoir les compétences du PFPD. Il doit non seulement contrôler le respect des exigences légales. En cas de violation, il doit aussi pouvoir prendre les mesures adéquates qui s'imposent et le cas échéant prononcer des sanctions. L'effectivité de la surveillance nécessite des ressources, qui aujourd'hui sont insuffisantes (voir aussi paragraphe 12.1 du présent rapport) et des pouvoirs de décisions. A l'instar d'autres autorités de protection des données en Europe et d'autres autorités de surveillance en Suisse, par exemple la Commission fédérale de la concurrence, il serait souhaitable que le PFPD soit doté du pouvoir de prononcer des sanctions. En outre, un droit de recours contre les décisions des organes fédéraux, similaire à celui prévu dans la loi sur la protection des données du canton de Glaris, pourrait être introduit.

1.2 EGouvernment

1.2.1 Efforts visant à introduire un identificateur fédéral de personnes

Un numéro arrêté à vie pour tous les citoyens et habitants suisses entraîne un gain d'efficacité dans la mise en relation et l'échange d'informations sur les personnes concernées. Le même gain d'efficacité peut a priori contribuer aussi bien à des activités à connotation positive, qu'à d'autres tenues pour dangereuses, voire abusives. Pour cette raison, nous revendiquons au même titre que le spécialiste du droit constitutionnel Giovanni Biaggini des définitions claires sur les finalités d'un éventuel identificateur de personnes.

Dans notre 9ème rapport d'activités (paragraphe 10.2), nous avions mentionné que l'introduction d'un identificateur de personnes en relation avec l'harmonisation des registres selon l'art. 65, al. 2 cst. constitue la question centrale pour la protection des données. Notre critique n'est pas dirigée contre l'introduction d'un numéro en soi, mais contre l'imprécision de son usage prévu et en particulier contre le fait qu'un numéro créé dans le cadre d'un projet statistique doit être introduit dans des registres qui, par définition, sont destinés à des fins administratives.

Il est vrai, selon les instances compétentes, que rien n'a été décidé au niveau politique en ce qui concerne un identificateur de personnes depuis le rapport d'activités de l'année dernière.

Ces instances ne semblent toutefois pas non plus particulièrement intéressées à une discussion politique. En effet, dans le communiqué de presse publié à l'occasion de la consultation relative à la loi fédérale sur l'harmonisation des registres de personnes, pas un seul mot n'est consacré à un identificateur de personnes. Par contre – et ceci nous paraît contestable – la question suivante est formulée dans la lettre d'accompagnement adressée aux organisations intéressées: «Quel genre d'identificateur de personnes préféreriez-vous en principe: un identificateur destiné à des fins administratives dans le domaine du contrôle des habitants conformément aux projets de cyberadministration de la Confédération et que la statistique pourrait utiliser conjointement ou un identificateur séparé ne pouvant servir qu'à des fins statistiques exclusivement?»

Dans divers projets relatifs à la cyberadministration, prévaut une «hypothèse de travail» selon laquelle un identificateur de personnes fédéral coordonné doit être introduit dans les registres administratifs. Sur la base de cette hypothèse, des jalons sont posés dans divers projets administratifs en matière de cyberadministration, ce qui en fin de compte crée aussi des contraintes. Il n'a nullement été tiré au clair quels effets cette infrastructure en voie de formation aura pour la protection de la personnalité. Une appréciation des conséquences n'a pas non plus été effectuée par les organes responsables.

Le fait qu'un identificateur de personnes purement statistique n'a absolument pas sa place dans les registres administratifs semble tout aussi oublié que la déclaration de l'Office fédéral de la statistique même selon laquelle la mise en relation des registres administratifs par un NIP «ne correspond pas à la culture politique en Suisse».

Un rapport d'expertise relatif aux barrières de droit constitutionnel pour un éventuel identificateur de personnes, dont nous avons confié le mandat à Giovanni Biaggini (professeur de droit public et administratif à l'université de Zurich), aboutit à la conclusion que la proportionnalité de l'emploi d'un tel code ne peut être examinée qu'en fonction d'objectifs mieux déterminés. Par conséquent, un identificateur de personnes ne peut être introduit dans certains registres administratifs que si cela est justifié par des motifs concrets dans le cadre de transactions administratives. La question de savoir si d'éventuels gains d'efficacité dans le domaine administratif l'emportent sur les risques en matière de protection de la personnalité ne peut être examinée que dans un contexte d'objectifs plus concrets et plus précisément définis.

1.2.2 Guichet virtuel, vote électronique et harmonisation des registres

Dans le domaine de la cyberadministration, le Préposé fédéral à la protection des données se trouve confronté à une multitude de projets dont certains poursuivent des buts imprécis ou franchement discutables. Le problème principal est que les organisations de projet concernées ne disposent ni des connaissances, ni de la sensibilité requises en matière de protection des données.

Dans notre 9ème rapport d'activités (paragraphe 1.1), nous avions relevé que les exigences de la sécurité et de la protection des données ne pourraient être formulées que lorsqu'il sera clair quelles transactions seront effectuées à ce guichet virtuel et par quels acteurs. Nous n'avons toujours pas obtenu plus de clarté dans ce domaine. Les trois sous-projets «Authentication», «Tracking» et «Payment» regroupés sous le titre moderne de «Web Services» concernent pourtant des éléments qui devraient contenir des informations extrêmement précises à cet égard dans leurs spécifications. Pour un projet d'une telle envergure et d'une telle sensibilité, il va de soi que les connaissances concernant la protection des données doivent se trouver au sein même de l'organisation du projet. C'est la seule façon pour la direction du projet d'assumer sa responsabilité et de garantir que les points sensibles seront identifiés et que les bonnes décisions seront prises lors des nombreuses séances de groupes de travail.

En ce qui concerne le vote électronique, nous avions retenu dans notre 9ème rapport d'activités (paragraphe 1.1) que les défis qui découlent du conflit d'intérêts entre le secret du vote et la nécessité de pouvoir retracer l'opération ne peuvent pas être considérés comme étant résolus à l'heure actuelle. Il faut relever qu'aucune analyse fondée des risques liés au vote électronique n'a été effectuée jusqu'ici au niveau suisse. C'est vraisemblablement la complexité technique du vote électronique qui fait que toutes les appréciations de risque qui ont été effectuées jusqu'ici ont porté exclusivement sur l'aspect technique. Les risques pour la démocratie en soi, qui touchent à la confiance du citoyen dans des institutions et des procédures qui fonctionnent bien, n'ont pas été examinés. Le thème «Vote électronique» a d'ailleurs été au centre du congrès «Informatique juridique» de cette année. La documentation de ce congrès (Congrès 2002 d'informatique juridique, Muralt Müller Hanna, Auer Andreas, Koller Thomas (éditeurs), Berne 2003, ISBN 3-7272-2162-3) examine divers aspects du vote électronique sous un angle critique. Etant donné que le vote électronique se trouve encore dans une phase d'essai précoce, une harmonisation des registres des électeurs à grande échelle telle qu'elle est revendiquée dans ce contexte par divers milieux, pose de sérieux problèmes du point de vue de la protection des données.

2. Protection des données – questions d'ordre général

2.1 Protection et sécurité des données

2.1.1 Sécurité du système sans la publication du code source (logiciels Open Source / logiciels libres)

Dans un environnement dans lequel les exigences envers la protection et la sécurité des données sont élevées, il est absolument nécessaire que le code source soit accessible ou qu'il soit publié. Il importe de pouvoir reproduire chaque opération d'un traitement afin de minimiser ou d'exclure les éventuels risques et dangers.

Pour la majorité des logiciels standards (applications et systèmes d'exploitation) utilisés de nos jours, le code source n'est pas publié. Les utilisateurs possèdent uniquement le programme compilé sans savoir comment celui-ci a été écrit ou programmé. Cette méthode présente certainement l'avantage pour l'éditeur du logiciel de ne pas devoir dévoiler à ses concurrents comment il a construit son logiciel. Il peut ainsi se procurer un avantage compétitif non négligeable. Pour la sécurité des données et donc également pour la protection des données, ce manque de transparence présente cependant des inconvénients. Jusqu'ici, la confiance en ces produits est encore plus ou moins donnée. On ne peut cependant jamais être sûr qu'un logiciel ne comporte pas de porte dérobée (backdoor) qui exécute des fonctions dont l'utilisateur ou l'exploitant n'a aucune connaissance. Il est en outre impossible de vérifier si le programme est entièrement exempt d'erreurs. Pour augmenter la protection et la sécurité des données, on choisit de nos jours souvent l'approche qui consiste à retenir le logiciel d'un fournisseur, mais de ne pas utiliser le logiciel de chiffrement que celui-ci propose. On utilise plutôt un autre logiciel de chiffrement dont le code source a été publié. Un des avantages des logiciels libres (Open Source Software) est que le code source est librement accessible et peut donc être examiné par n'importe quel expert. Une telle publication permet également de découvrir plus rapidement d'éventuelles erreurs, pour autant que le code source soit vraiment analysé. D'un autre côté, il faut être conscient du fait que le volume des lignes de code source est souvent si énorme que l'on ne peut pas forcément admettre que les programmes aient été entièrement analysés. On peut néanmoins présumer que les éditeurs de logiciels tendent plutôt à ne pas publier le code source dans les cas où ils ont intégré une porte dérobée dans leur logiciel. Vous trouverez des informations détaillées ainsi que des définitions de notions relatives aux logiciels libres (Open Source Software) sur les sites web suivants:

http://www.opensource.org; http://www.ifross.de/

Nous avons déjà attiré l'attention dans le cadre des procédures de chiffrement sur le fait qu'il fallait utiliser un procédé de chiffrement publié pour des raisons relevant de la protection et de la sécurité des données. Ceci est également valable pour l'utilisation d'autres logiciels. Si le code source d'un logiciel n'est pas librement accessible, la protection des données ne peut pas être garantie, ce qui peut devenir très problématique dans des environnements sensibles. On se rend compte de cet état de fait entre autres lorsqu'on prévoit de réaliser des systèmes permettant le vote par voie électronique (e-voting) qui soient conformes aux exigences de la protection des données. D'un côté, les votants ont le droit de voter de manière anonyme, d'un autre côté il doit être possible de vérifier si le votant en question a déjà voté une fois pour éviter qu'il ne le fasse une deuxième fois. Il faut également garantir qu'un «oui» sera toujours reconnu comme tel par le système. C'est la raison pour laquelle il est important que le code source soit divulgué afin qu'il puisse être analysé par des experts. Il est également envisageable dans certains cas spéciaux, où une publication à grande échelle risquerait à son tour de créer des problèmes de sécurité, que l'examen de certaines parties du code source ne puisse être effectué que par un cercle restreint de personnes. La divulgation du code source permet de voir quelles sont les fonctions exécutées par le système et de suivre le flux des informations. Des portes dérobées, qui permettraient par exemple de manipuler les votes enregistrés, pourraient être exclues avec une haute probabilité par le recours à un tel procédé. Les aspects de protection et de sécurité des données jouent un rôle essentiel et constituent un objectif impératif pour des systèmes aussi sensibles, ils doivent donc impérativement être respectés ou appliqués pour qu'un tel système puisse être mis en exploitation.

2.1.2 Effacement physique de données sur supports magnétiques

Lorsque l'on supprime des données sur un support de données en utilisant les fonctions du système d'exploitation, ces données peuvent être récupérées avec plus ou moins d'effort. Ceci est même possible lorsque le support de données a été reformaté. Du point de vue de la protection des données, ceci pose problème – surtout dans l'administration fédérale – étant donné que la LPD stipule que les données personnelles qui ne sont plus utilisées doivent être détruites. Certains éditeurs de logiciels proposent des outils qui permettent de procéder à un effacement physique des données.

Conformément à la loi fédérale sur la protection des données, les données personnelles qui ne sont plus utilisées doivent être – surtout dans l'administration fédérale – soit rendues anonymes, soit détruites, à moins qu'elles ne doivent être conservées à

titre de preuve ou par mesure de sûreté ou déposées aux Archives fédérales. Ni la suppression traditionnelle des données, ni le formatage du support de données ne remplissent les exigences de la loi sur la protection des données en ce qui concerne la destruction des données. Par destruction on entend un effacement des données personnelles qui exclut toute reconstruction subséquente. Les instructions communément utilisées dans les systèmes informatiques ne font que marquer les données comme étant supprimées sans pour autant les effacer physiquement, ce qui signifie que ces données peuvent être récupérées en utilisant des outils appropriés, pour autant que la partie concernée du support de données n'ait pas déjà été réutilisée pour mémoriser d'autres données. Quant à l'instruction «format», elle peut être annulée par l'instruction «unformat» ce qui fait que cette instruction ne peut pas non plus être considérée comme sûre. Le formatage de bas niveau (format /U) de DOS recrée les secteurs et les pistes d'un disque dur et les remagnétise en y inscrivant une configuration binaire. Les avis divergent sur la qualité de ce procédé d'effacement. Alors que les uns affirment que les données sont irréversiblement détruites à l'issue d'une telle procédure, d'autres soutiennent qu'il existe des utilitaires permettant de récupérer les données initiales. Il existe aujourd'hui, notamment pour les systèmes d'exploitation DOS et Windows, des outils qui permettent d'effacer les données de manière à ce qu'elles ne puissent plus être reconstruites. Pour ce faire, ces utilitaires magnétisent la partie effacée d'un disque avec une ou plusieurs configurations binaires de manière à ce qu'il ne soit plus possible de récupérer les données initiales. Le logiciel PGP (Pretty Good Privacy) indique par exemple qu'il effectue:

- 3 passages d'écrasement pour les usages privés
- 10 passages d'écrasement pour les usages commerciaux
- 18 passages d'écrasement pour les usages militaires
- 26 passages d'écrasement lorsqu'une sécurité maximale est exigée.

Des entreprises professionnelles, spécialisées dans la récupération de données, ont réussi à reconstruire des données qui ont été écrasées neuf fois de suite. Il semble que la configuration binaire utilisée joue un rôle non négligeable dans la procédure d'effacement. Un aspect dont il faut également tenir compte est qu'il faut prévoir le temps nécessaire pour effectuer les multiples passages d'effacement. Comme nous l'avons déjà mentionné plus haut, de tels outils sont disponibles surtout pour les systèmes d'exploitation DOS et Windows. Pour les autres systèmes d'exploitation, il est parfois nécessaire d'appliquer d'autres procédés. Comme procédés alternatifs, les données peuvent également être effacées en appliquant des champs magnétiques puissants ou par destruction physique des supports de données. Les deux procédés occasionnent cependant – si on les compare aux mesures décrites ci-dessus –

la plupart du temps des frais très élevés. C'est pourquoi il est indiqué pour les projets de poser déjà dans le cahier des charges la question aux fournisseurs comment ils comptent garantir la «destruction physique irréversible» des données. Si une solution de destruction physique des données doit être trouvée après coup (après les phases de planification du projet et après l'appel d'offres), elle occasionnera le plus souvent plus de frais que si on avait étudié la question au début du projet déjà.

2.1.3 Dépouillement des fichiers de journalisation de serveurs web

Un des principes de la protection des données demande que le traitement soit limité au strict minimum des données personnelles qui sont vraiment nécessaires pour l'accomplissement de la tâche. Lors du dépouillement de fichiers de journalisation de serveurs web, il n'est en règle générale pas nécessaire de tenir compte de l'adresse IP (une donnée personnelle permettant l'identification). Une pseudonymisation de cette adresse permettrait d'éliminer le rapport direct avec la personne et de mettre les fichiers de journalisation à disposition des analystes sous une forme anonymisée.

De nos jours, un grand nombre de services et d'entreprises publics utilisent Internet pour mettre des informations à disposition du grand public. Il est certainement intéressant pour le fournisseur des informations de pouvoir constater quelles sont les informations qui ont été consultées par les personnes intéressées ou même de savoir dans quel ordre ces informations ont été appelées. Pour atteindre cet objectif, il n'est cependant pas nécessaire de connaître l'adresse IP, une donnée qui permet dans certains cas d'identifier la personne qui a accédé au site ou au moins son fournisseur d'accès Internet. Du point de vue de la protection des données, il ne suffit pas que le service qui enregistre les fichiers de journalisation et l'organe qui met à disposition les informations sur Internet conviennent par contrat que les fichiers de journalisation ne peuvent être dépouillés qu'à cette fin. Les systèmes doivent, du point de vue technique et organisationnel, être conçus de manière à ce qu'ils rendent impossible d'éventuels abus ou des actes ne correspondant pas à la finalité.

La protection des données part du principe que seul le minimum de données personnelles qui sont nécessaires pour l'accomplissement de la tâche doit être mis à disposition pour le traitement de données. Dans le cas présent, nous sommes d'avis qu'une bonne solution consisterait à anonymiser ou éventuellement pseudonymiser les fichiers de journalisation. Dans la mesure où l'exploitant du site web transmet les fichiers de journalisation de manière anonymisée ou pseudonymisée aux services spécialisés, nous n'avons aucune objection à formuler du point de vue de la protection des données. Dans les cas où il est nécessaire de disposer de l'adresse IP pour

reconstituer l'ordre chronologique du traitement, on peut par exemple remplacer ces adresses IP par des séquences de caractères non interprétables et toujours identiques pour éviter que ces fichiers fournissent des indications permettant d'identifier la personne. Il va de soi que l'algorithme doit être conçu de manière à être univoque, mais pas biunivoque. Cela signifie qu'une même source est toujours convertie en une même cible sans qu'il soit cependant possible depuis la cible de retrouver la source correspondante. La solution idéale serait que les systèmes attribuent directement des numéros pseudonymisés, c.-à-d. que les journaux soient écrits sous cette forme évitant ainsi de devoir après coup procéder à une pseudonymisation des données identifiantes. Il doit néanmoins être possible dans des cas isolés de procéder à une dépseudonymisation des adresses. Si nécessaire, celle-ci doit impérativement être effectuée en respectant le principe des quatre yeux (séparation des tâches). Il y a lieu de relever qu'un pseudonyme sûr ne peut être créé que si les données de base utilisées sont elles-mêmes sûres. Comme chacun sait, il est très facile de modifier une adresse IP, ce qui signifie qu'il n'est pas très judicieux de prendre cette donnée de base comme point de départ.

2.1.4 Problèmes de protection des données posés par les photocopieurs et imprimantes modernes

Ces derniers temps, les photocopieurs ont subi une évolution pour devenir de vrais appareils multifonctions disposant de beaucoup d'«intelligence» propre. Cette évolution a également soulevé des risques en ce qui concerne la protection des données. Chaque fois qu'un document est numérisé, il se retrouve en mémoire pendant un certain laps de temps. Ces appareils peuvent en outre être intégrés dans un réseau informatique. Voilà une raison suffisante pour les étudier de plus près du point de vue de la protection des données.

Nombreux sont les utilisateurs qui ignorent que les photocopieurs numériques modernes qu'ils utilisent quotidiennement mémorisent une copie numérique de chaque document, la quelle peut rester disponible pour une période prolongée. Ceci peut mener à une accumulation énorme de documents confidentiels. Le risque d'un accès illicite ne doit par conséquent pas être négligé.

Un photocopieur numérique ne reproduit pas simplement un document, il le numérise d'abord ce qui permet d'effectuer divers traitements subséquents. Ces appareils peuvent également être connectés à un réseau d'entreprise et souvent ils sont également équipés de fonctions de télécopie. Toutes ces fonctions annexes nécessitent que le document soit temporairement stocké dans la mémoire vive (volatile), souvent aussi sur un disque dur.

En fonction du type d'appareil et des réglages effectués, les données ainsi mémorisées sont automatiquement effacées après chaque travail d'impression, après chaque réenclenchement de l'appareil, après un intervalle de temps prédéfini ou même jamais. Certains appareils permettent à l'utilisateur de supprimer manuellement les données. Rien que l'usage de la fonction qui permet d'imprimer une copie du dernier document traité peut déjà avoir des conséquences catastrophiques.

Une personne non autorisée ne doit disposer d'aucune possibilité de retirer de l'appareil un support de données (en règle générale un disque dur) qui contient des documents copiés/scannés. Lorsque le personnel technique d'entretien procède à l'échange d'un disque dur, il doit appliquer les mêmes précautions de sécurité que celles qui valent pour un ordinateur: les données doivent être supprimées de manière irrévocable avant que le support de données ne sorte de l'entreprise.

Un autre risque est celui qu'une personne puisse accéder à l'appareil par l'intermédiaire du réseau (pour autant que celui-ci soit présent), depuis un poste de travail éloigné. Il importe donc de mettre en place des consignes d'accès très strictes pour ces cas. Certains constructeurs proposent en option des solutions accessoires offrant une sécurité accrue. Il est impératif que tous les collaborateurs qui utilisent des photocopieurs numériques aient été instruits sur les fonctions de l'appareil ainsi que sur les risques existants afin qu'ils puissent adapter leur comportement en conséquence.

Il importe que l'on veille déjà lors de l'évaluation d'appareils numériques de copie à ce qu'ils puissent être exploités (au niveau matériel et logiciel) de manière à ce que les exigences de l'entreprise en matière de protection et de sécurité des données puissent être entièrement respectées. La responsabilité en incombe à l'exploitant en sa qualité de maître du fichier. La loi sur la protection des données exige expressément que les données personnelles soient protégées, par des mesures techniques et organisationnelles appropriées, contre tout traitement non autorisé. Les utilisateurs devraient renoncer à photocopier des documents sensibles sur un appareil dont ils ne savent pas comment les données y sont traitées et, en particulier, quelles possibilités d'y accéder existent.

2.1.5 La «Trusted Computing Platform Alliance» (TCPA) et la protection des données

Les notions de sécurité (security) et de confiance (trust) sont très fréquemment utilisées par les fournisseurs de produits et de prestations de service informatiques dans leurs communications mercatiques. Le fait qu'il soit souvent difficile – si elles ne sont pas mieux précisées – de saisir le sens exact de ces notions qui sonnent si positives, nuit malheureusement à la clarté.

Depuis des années, un grand nombre de sociétés regroupant les plus importants fournisseurs et constructeurs de matériel et de logiciels pour PC s'engagent pour un projet dont l'objectif précis n'est pas vraiment clair, en tout cas pas au premier abord. Les divers aspects du projet TCPA ainsi que le fait qu'il suscite non seulement l'intérêt des fournisseurs cités plus haut, mais surtout celui de l'industrie des loisirs (musique et film) nous mène à conclure qu'un des principaux objectifs de ce projet est de développer les moyens techniques de protection contre la copie d'œuvres protégées par le droit d'auteur. A première vue, ceci ne semble donc pas relever avant tout du domaine de la protection des données; si on y regarde cependant d'un peu plus près, on constate que la protection des données pourrait très bien être concernée par ce projet. Nous ne pouvons pas dans le cadre de ce rapport passer en revue les énormes conséquences potentielles de la surveillance qui serait mise en place par le mécanisme central de TCPA, le «Digital Rights Management». Nous devons cependant rendre attentif au fait que, selon les informations que nous possédons à l'heure actuelle sur TCPA, l'objectif est de vendre à l'avenir aux utilisateurs une infrastructure contenant des fonctions de sécurité que ceux-ci ne peuvent ni contrôler eux-mêmes, ni comprendre en détail. Une telle démarche créerait non seulement un manque de transparence flagrant, mais empêcherait en fin de compte le droit du consommateur à l'autodétermination individuelle en matière d'information. C'est la raison pour laquelle les Préposés à la protection des données de la Fédération et des Länder d'Allemagne ont pris une résolution à l'occasion de leur 57ème Conférence (http://www.lfd.m-v.de/beschlue/ent57.html) demandant que les fournisseurs de technologies d'information et de communication produisent et développent leurs matériels et logiciels de manière à ce que les utilisateurs et des tiers indépendants soient en mesure à tout moment de se convaincre de l'efficacité des mesures de sécurité. Nous soutenons également cette demande.

Dans une des premières analyses – et d'ailleurs une des plus approfondies à ce jour – effectuées sur TCPA/Palladium (la version TCPA de Microsoft) (cf. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html), Ross Anderson – un des meilleurs experts dans le domaine des technologies de sécurité – a très bien résumé la question essen-

tielle de ce projet: il pose la question rhétorique de savoir si cela n'est pas une bonne chose de disposer d'une meilleure sécurité sur les PC. Et, quasiment en guise de réponse, il pose ensuite la question essentielle: «Sécurité pour qui?». Voici quelques-uns des éléments de la réponse donnée par Anderson: ni le problème des virus informatiques, ni celui de notre submersion par du courrier électronique publicitaire non sollicité (spam) ne sera résolu par TCPA. Cette nouvelle technologie ne limitera pas non plus les atteintes aux droits de la personnalité ou à la protection des données. Les intérêts en matière de sécurité qui sont protégés en premier lieu par TCPA ne sont pas ceux des utilisateurs de PC, mais ceux des vendeurs de PC, des éditeurs de logiciels et de l'«industrie des contenus» (musique, film, jeux).

2.1.6 Formation complémentaire des préposés à la sécurité informatique de la Confédération en matière de protection technique des données

Les préposés à la sécurité informatique de la Confédération (ISBO) bénéficient désormais d'une formation complémentaire sur les mesures techniques et organisationnelles de protection des données. Les thèmes abordés gravitent autour de la pseudonymisation/anonymisation des données personnelles, leur chiffrement à la source, les conditions de traitement des nombreux fichiers journaux, ainsi que le devoir d'annonce et l'exercice du droit d'accès. Cet éclairage particulier permet d'élargir les mesures habituelles de sécurisation des données.

Les préposés à la sécurité informatique des unités organisationnelles (ISBO) de la Confédération ont la possibilité de suivre régulièrement des journées de formation sur les nouveautés en matière de sécurité informatique. Nous avons proposé de compléter cette offre par un éclairage particulier sur les mesures techniques et organisationnelles de protection des données. Les principes de proportionnalité et de finalité imposent des méthodes de non-production ou d'économie des données, qui contribuent auxiliairement à réduire la taille et la complexité des applications et des bases de données. A cet égard, il faut relever que les innombrables fichiers journaux foisonnant de manière quasi anarchique en marge des applications et systèmes informatiques doivent absolument satisfaire à ces exigences. Les différentes variantes et conditions de pseudonymisation et anonymisation de données personnelles sont ensuite présentées et expliquées en détail. L'accent est alors mis sur le principe du chiffrement des données sensibles à la source et non pas exclusivement lors de leur mémorisation ou de leur transmission. L'avantage réside dans la protection originelle dont ces données bénéficient, notamment par rapport aux ingénieurs du système ou aux

copies sur support d'archivage. Le problème du maintien de la disponibilité des données chiffrées conduit alors à aborder les questions cruciales de dépôt centralisé des clés utilisées, ainsi que de clé additionnelle générique de déchiffrement. Une clarification de la finalité exacte de telles mesures, qui ne peuvent être prises qu'en absolue transparence par rapport aux personnes concernées, permet en principe d'évaluer leur bien-fondé. D'autres principes spécifiques de protection des données comme l'exigence d'une routine d'interrogation pour l'exercice du droit d'accès par la personne concernée ou l'obligation d'annonce par le maître de fichier sont enfin rappelés. Il est important de remarquer la complémentarité des mesures de sécurité et de protection des données, tout en gardant à l'esprit qu'une sécurité élevée des données ne garantit pas automatiquement une bonne protection des données (ex: collecte abusive de données personnelles mémorisées sous forme chiffrée!), alors qu'une haute protection des données est impossible sans une sécurité optimale des données (mots de passe, antivirus, firewalls, etc). Il faut d'ailleurs rappeler que la sécurité de l'information est le résultat d'un équilibre de sécurisation physique, technique, organisationnelle et humaine. L'expérience faite au cours de cette première année de collaboration démontre à l'évidence que les ISBO sont intéressés par les méthodes spécifiques de protection des données, puisqu'elles leur permettent de compléter leurs compétences avérées en sécurité des données.

2.2 Autres thèmes

2.2.1 La banque de données nationale pour le sport

L'Office fédéral du sport a mis sur pied une banque de données nationale pour le sport dans le cadre de la réorganisation du programme Jeunesse et Sport (J+S). Elle contient des données sur les responsables de cours et permet en outre d'administrer et de gérer les cours offerts par J+S au niveau national.

L'Office fédéral du sport (OFSPO) avait reçu mandat de réexaminer en profondeur le programme J+S et de l'adapter aux besoins actuels. Ce mandat prévoyait entre autres la création d'une banque de données nationale pour le sport (BDNS). Celle-ci devra permettre la gestion informatisée au niveau fédéral des données relevant du domaine de la formation des jeunes et de la formation des cadres de J+S, ainsi que des cours J+S. La BDNS remplacera les divers programmes informatiques utilisés jusqu'ici par les cantons.

Nous avons assisté l'OFSPO dans la mise en place de la base légale servant de fondement à la banque de données nationale. Avec l'OFSPO également, nous avons tout particulièrement veillé à réglementer de manière claire et transparente la responsabilité du traitement des données, les nombreuses autorisations d'accès et le volume des données traitées. Les deux annexes à l'ordonnance contiennent la liste complète des donnés et réglementent de manière exhaustive les autorisations d'accès des différentes unités d'organisation.

Non seulement l'ordonnance détermine de manière claire quelles autorités et quels organisateurs de manifestations sportives auront accès aux données personnelles de la BDNS, mais elle établit également à quelles conditions les données personnelles relevant du domaine de J+S pourront être communiquées à des tiers.

2.2.2 Contrôle à l'entrée d'un club de fitness

Seules les personnes qui acceptaient de se faire photographier pouvaient contracter un abonnement et devenir membre d'un club de fitness. Un flou subsistait néanmoins sur l'utilisation prévue de la photographie en question. Nous avons émis une recommandation sur cette pratique que la gérante du club a acceptée. Le texte de cette recommandation se trouve au paragraphe 13.7.1.

Les personnes qui désiraient devenir membre du club de fitness ne pouvaient contracter un abonnement qu'à la condition d'accepter de se faire photographier. Cette photo était mise dans le fichier des membres à des fins d'identification et de contrôle, aux dires de la direction du club. Les conditions générales précisaient uniquement à ce propos que la personne concernée devait prendre connaissance du fait qu'une photographie allait être prise d'elle à usage interne. L'aspect indéfendable de la chose était que le club n'indiquait pas ouvertement les détails du traitement des données. Ainsi, nul ne savait de quelle manière la photographie était utilisée et quel était le but de ce traitement de données outre le contrôle visuel.

Lorsque nous avons fait remarquer au club de fitness que ce genre de pratique n'était pas conforme aux principes de la protection des données, celui-ci a objecté, en nous renvoyant aux conditions générales, que les photographies étaient faites avec le consentement exprès des personnes concernées. En outre, il s'appuyait sur le motif justificatif de l'intérêt prépondérant à effectuer ce traitement de données en relation directe avec la conclusion ou l'exécution d'un contrat.

Dans notre recommandation, nous avons expliqué au club de fitness que la personne concernée ne peut donner un consentement valable en droit que si elle a été infor-

mée ouvertement et complètement des détails du traitement de données. Il est toutefois impossible de déduire un consentement d'une clause formulée de manière imprécise dans les conditions générales. Nous avons en outre montré pourquoi même en présence d'un contrat, tous les traitements de données n'étaient pas admis sans limite. Ainsi, le principe de la proportionnalité requiert que seul le traitement de données objectivement nécessaire pour atteindre un objectif déterminé soit autorisé et qu'il entretienne un rapport raisonnable avec l'atteinte à la personnalité.

Ainsi, il suffit que le futur membre justifie de son identité, en plus de son abonnement, par la présentation d'un document officiel muni d'une photo d'identité, par exemple sa carte d'identité. Une autre solution serait de remettre aux membres une carte d'abonnement comportant une photographie de l'ayant droit et que chaque membre devrait montrer à l'entrée. Ces deux mesures permettent une identification claire de l'ayant droit et porte une atteinte moindre à la sphère personnelle de la personne concernée qu'un fichier de photographies.

Dans notre recommandation, nous avons aussi demandé au club de fitness de signaler de manière adéquate, expresse et concrète aux personnes concernées, avant la conclusion du contrat, le but et l'étendue du traitement de données ou de leur donner la possibilité de contracter un abonnement sans que cela implique l'intégration de leur photographie dans un fichier.

Le club de fitness a accepté notre recommandation. Désormais, les clients sont informés de manière claire et complète dans les conditions générales, remaniées par la direction, du traitement des données les concernant.

2.2.3 Le principe du libre-service dans les magasins de photo est illicite

De plus en plus de professionnels du développement photo pratiquent le principe du libre-service. Les clichés tirés sur papier sont dans ce cas accessibles à tous. Chacun peut regarder et même prendre des photos qui ne le concernent pas. Par le biais de mesures organisationnelles appropriées, le commerçant est tenu de veiller à ce que seules les personnes autorisées puissent avoir accès aux photos.

Nous sommes régulièrement contactés par des personnes qui apportent leurs films à développer soit à un grand distributeur, soit à un détaillant ou même un magasin de photo et qui, lorsqu'ils viennent chercher leurs clichés, ont la surprise de devoir les chercher parmi une multitude d'autres enveloppes contenant également des photos. Chaque enveloppe porte le nom et l'adresse de la personne autorisée et contient les photos ainsi que les négatifs. Pour les curieux, rien n'est plus facile que de sortir une

enveloppe quelconque, de l'ouvrir et de regarder les photos d'autres personnes et même de se les approprier. Des tests effectués par la Fondation pour la protection des consommateurs ont montré que dans certains cas même, des personnes non autorisées pouvaient «acheter» des enveloppes tout entières.

Le nom, l'adresse et les photos sont des données personnelles au sens de la loi sur la protection des données. Le commerçant qui tient les photos développées à la disposition de sa clientèle doit à cet égard respecter les principes de la protection des données et traiter de manière confidentielle les données personnelles qui lui sont confiées. Il est ainsi tenu de veiller à ce que les données personnelles soit protégées contre tout traitement non autorisé par des mesures organisationnelles appropriées. En laissant tout simplement les enveloppes contenant les clichés tirés sur papier – négatifs compris – dans une caisse où toutes les personnes entrant dans son magasin peuvent se servir, le commerçant ne respecte pas cette prescription. Il porte une atteinte illicite à la personnalité de ses clients et enfreint la loi sur la protection des données.

Par conséquent le principe du libre-service appliqué à la remise des développements de photos est illicite. Le commerçant doit veiller à ce que les enveloppes contenant les clichés soient conservées dans un endroit non accessible à tout le monde et que seul le personnel autorisé puisse avoir accès à ces mêmes enveloppes. Avant de remettre les photos développées, le personnel doit s'assurer qu'elles sont bien remises à la personne à qui elles appartiennent en vérifiant que le coupon de contrôle numéroté correspond bien à la marchandise remise.

2.2.4 Enquête du TCS auprès de ses membres

La qualité de membre d'une association ne contraint pas à communiquer au comité de cette association toutes les données concernant sa personne. Si les données requises n'entretiennent pas un rapport direct avec l'objectif de l'association, le comité doit au préalable informer les membres du but dans lequel elle entend utiliser les données et préciser que la communication de données personnelles est facultative puisqu'elles n'ont pas de rapport direct avec la raison d'être de l'association.

Le TCS a demandé à ses membres, sans plus d'informations, de remplir un questionnaire. Ce dernier contenait entre autres des questions sur le ou la partenaire (nom, prénom, date de naissance, nationalité), sur les enfants à charge, sur le revenu brut du ménage, sur les passe-temps favoris, etc. De nombreux membres du TCS se sont adressés à nous pour savoir si ce genre de collecte d'informations par le TCS est licite.

L'exploitation de ces questionnaires dûment remplis et renvoyés fournit au TCS des données détaillées sur ses membres. Le TCS traite dans ce cas des données personnelles et est donc tenu de respecter les principes de la protection des données. Nous avons exposé en détail au TCS la raison pour laquelle sa manière de procéder n'est pas conforme – à divers égards – aux principes de la protection des données. Par exemple, le principe de transparence (principe de la bonne foi) requiert une information franche et exhaustive sur le but et le volume des données personnelles traitées. Cela implique aussi que l'on informe la personne questionnée si ses données personnelles sont transmises à des entreprises tierces et – si tel est le cas – à qui et dans quel but. Le principe de la proportionnalité n'autorise que le traitement des données personnelles réellement nécessaires pour atteindre le but indiqué lors de leur collecte. Le principe de finalité lui aussi oblige le maître du fichier à ne traiter les données personnelles que dans le but indiqué lors de leur collecte.

Par le biais de ce questionnaire, le TCS reçoit de ses membres des informations très détaillées qui n'entretiennent pas de rapport direct avec le but poursuivi par l'association. Il convient donc d'attirer au préalable l'attention des membres sur ce fait et souligner expressément que la participation au questionnaire demeure facultative.

Après notre intervention, le TCS s'est déclaré prêt à remédier à cette situation et à publier un article dans sa revue afin d'informer ses membres avec précision sur cette enquête (entre autres l'objectif poursuivi, le volume des données traitées, la transmission éventuelle à des tiers, la durée de conservation, le droit de révocation, la responsabilité de l'enquête, etc.).

Le TCS a également assuré qu'il élaborera un concept de protection des données. Il entend de cette manière garantir en tout temps à ses membres un traitement des données personnelles conforme aux principes de la protection des données.

3. Justice/ Police/ Sécurité

3.1 Affaires de police

3.1.1 Données biométriques contenues dans des documents d'identité

L'introduction de données biométriques dans les documents d'identité doit respecter les principes généraux de protection des données, notamment le principe de finalité et celui de proportionnalité. Cela signifie que les buts poursuivis doivent être clairement définis et qu'il y a lieu d'analyser tous les autres moyens permettant d'atteindre ces objectifs. Dans le cas où l'introduction de données biométriques s'avérerait nécessaire et apte à atteindre les buts poursuivis, il faudra procéder à un choix des données biométriques à introduire dans les documents d'identité en fonction des risques d'atteinte à la personnalité.

Suite aux tragiques événements du 11 septembre 2001, les Etats-Unis font pression sur les autres Etats afin que ces derniers introduisent des données biométriques lisibles mécaniquement dans les passeports. Les ressortissants des Etats qui n'auront pas de données biométriques incorporées dans les documents d'identité ne pourront plus entrer (vraisemblablement dès la fin 2004) sur le territoire américain sans visa. Dans le cadre de l'introduction du nouveau passeport et de la nouvelle carte d'identité en Suisse, la question des données biométriques s'est posée. Une telle opération aurait nécessité une modification de la loi sur les documents d'identité et des adaptations techniques.

Avant d'introduire de nouvelles données biométriques (la photographie, la taille et la signature étant déjà des données biométriques) dans les documents d'identité, il est absolument nécessaire de définir les finalités des traitements envisagés: identifier le porteur du document, comparer avec une banque de données de recherche, enregistrer le contrôle ou l'entrée sur le territoire dans un fichier. La proportionnalité des mesures envisagées doit ensuite être analysée minutieusement. Il s'agit notamment d'évaluer tous les moyens permettant d'atteindre les buts définis et de ne retenir que ceux qui menacent le moins la personnalité des personnes concernées (ceux qui n'incluent pas de données sensibles ou qui ne permettent pas d'établir des profils de la personnalité par exemple). Si l'introduction de données biométriques s'avérait finalement nécessaire, il conviendra alors de choisir celles qui menacent le moins la personnalité. Une donnée biométrique qui permet de déduire des indications sur la santé ou sur la sphère intime est ainsi à exclure.

L'évolution au niveau international de la question de l'utilisation de données biométriques, notamment dans les domaines des transports aériens et de la lutte contre le terrorisme sera déterminante pour la position de la Suisse.

3.1.2 Mesures prévues en matière d'hooliganisme, de racisme, d'extrémisme et de terrorisme

Dans le cadre des mesures prévues contre le racisme et l'hooliganisme, il est envisagé de créer une banque de données «hooliganisme». Nous avons été invités à donner notre avis sur le projet de loi correspondant. D'autres mesures sont prévues dans les domaines du terrorisme et de l'extrémisme.

Le Conseil fédéral a décidé de scinder les projets législatifs en cours sur l'extrémisme de droite en deux volets. Le premier volet concerne le racisme et l'hooliganisme, le deuxième le terrorisme et l'extrémisme.

En ce qui concerne le premier volet, nous avons pu prendre position dans le cadre de la consultation des offices sur la nouvelle loi fédérale instituant des mesures contre le racisme et l'hooliganisme. Parmi les mesures prévues pour endiguer le racisme, cette loi prévoit entre autres la possibilité de confisquer du matériel de propagande. Une autre mesure de lutte contre le hooliganisme prévue par cette loi consiste à mettre sur pied un système d'information recueillant des données sur des personnes qui ont eu un comportement violent lors de manifestations publiques, notamment lors de rencontres sportives. Ce projet soulève un certain nombre de questions en ce qui concerne la protection des données. Nous avons pu conclure des explications accompagnant le projet de loi que les manifestations de violence spontanées ne devaient pas tomber sous le coup de cette loi, étant donné que celles-ci ne justifiaient pas une saisie des organes de protection de l'Etat. Nous avons partagé cet avis, tout en rendant attentif au fait qu'il fallait établir des critères précis permettant de dissocier les manifestations spontanées de violence des actions de violence organisées. Nous avons en outre relevé que la loi devait définir clairement quelles données personnelles pourraient être traitées dans le nouveau système d'information. C'est pour cette raison que nous avons jugé une partie de l'article du projet de loi relatif au système d'information comme étant bien trop vague et manquant de précision. Le système d'information doit aussi être clairement décrit dans la base légale. En conséquence, nous avons demandé que les catégories de données traitées ainsi que les autorités qui seront autorisées à accéder au système d'information soient mentionnées dans le texte de loi même. Le projet de loi prévoit en outre que les organisateurs d'une manifestation peuvent, dans certaines conditions, recevoir des données en provenance de la nouvelle base de données. Il est important dans ces cas de veiller à ce

que les données communiquées aux organisateurs soient effacées à la fin de la manifestation publique pour éviter que ces derniers puissent utiliser ces données personnelles pour créer leur propre fichier des hooligans.

En ce qui concerne le volet «terrorisme/extrémisme», il n'existe encore aucune proposition de modification législative. Nous avons eu la possibilité à ce sujet de prendre position dans une note de discussion adressée au Conseil fédéral. Tenant compte du fait qu'il n'existe pas encore de propositions tangibles, nos remarques à ce sujet ont eu un caractère plutôt général. Nous nous sommes expressément réservé le droit de prendre position plus en détail dès que des projets législatifs concrets nous auront été soumis.

3.1.3 Expériences avec le droit d'accès indirect

Le traitement des demandes d'accès indirectes en rapport avec la sécurité intérieure et la lutte contre le blanchiment d'argent n'a rencontré aucun obstacle. Par contre, les demandes concernant le crime organisé, le trafic illicite de stupéfiants, le faux-monnayage, la traite des humains et la pornographie ont rencontré bien plus de problèmes, liés à la nature même du système d'information JANUS. Quelques-unes des demandes ont en outre été portées devant la Commission fédérale de la protection des données.

Après avoir recensé dans la période 2001/2002 une augmentation nette du nombre de demandes pour le système de traitement de données relatives à la protection de l'Etat (ISIS) en application de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), le nombre de demandes a de nouveau diminué dans la période 2002/2003. A l'époque, cet accroissement était principalement dû aux traitements de données personnelles par le Service d'analyse et de prévention (SAP) de l'Office fédéral de la police (OFP) dans le cadre du Sommet du G8 à Gênes. Actuellement le nombre de demandes est à peu près comparable à celui des périodes 1999/2000 et 2000/2001. Par contre, le nombre des demandes d'accès indirectes fondées sur la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) a fortement augmenté. Ceci est vraisemblablement dû au fait que cette base de données est entre-temps mieux connue du public. Au total, le nombre des demandes d'accès indirectes est en légère baisse.

En ce qui concerne le traitement des demandes, la situation telle que nous l'avons décrite dans notre dernier rapport d'activités (9ème rapport d'activités 2001/2002, paragraphe 3.1.1) n'a pas beaucoup évolué. Ainsi, l'examen des demandes concernant le système ISIS a continué à s'effectuer sans problème. Ceci vaut également pour les demandes concernant le système GEWA du Bureau de communication en matière de

blanchiment d'argent. Pour les demandes de renseignement concernant le système JANUS, la situation a également très peu changé depuis notre dernier rapport d'activités. L'OFP n'a pas encore réussi à rectifier les irrégularités que nous avions mentionnées dans nos recommandations.

Finalement, il reste à relever qu'un certain nombre de personnes concernées ont porté leur cas (concernant aussi bien ISIS que JANUS et GEWA) devant la Commission fédérale de la protection des données.

3.2 Autres thèmes

3.2.1 Révision de la législation sur les étrangers

L'utilisation d'analyses génétiques dans le but d'identifier une personne ou dans le cadre du regroupement familial sera réglée dans la future loi fédérale sur l'analyse génétique humaine. La nécessité de procéder à de telles analyses n'étant toujours pas démontrée, leur usage est contraire au principe de proportionnalité. L'utilisation de la vidéosurveillance ou de systèmes de reconnaissance pour identifier des personnes ne pouvant pas entrer sur le territoire suisse et devant être prises en charge par les compagnies aériennes les ayant transportées heurte le principe de proportionnalité en raison du faible nombre de personnes visées. L'utilisation des même moyens à des finalités ne relevant pas du domaine des étrangers doit faire l'objet d'un examen plus approfondi et, si la nécessité est démontrée, être réglée dans le cadre de dispositions relevant de la police ou de la sécurité intérieure.

Contrairement au premier projet de loi sur les étrangers, celui soumis au Parlement ne mentionne plus le recours à des analyses génétiques dans le but d'identifier une personne ou dans le cadre du regroupement familial. Le Conseil fédéral ne renonce pas aux analyses génétiques, mais celles-ci seront réglées par la future loi fédérale sur l'analyse génétique humaine. La nécessité de procéder à des analyses génétiques pour accomplir les tâches relatives au droit sur les étrangers n'est pas démontrée. L'usage d'analyses génétiques dans ce contexte est ainsi contraire au principe de proportionnalité. La situation est identique pour le projet de loi sur l'asile également soumis au Parlement (voir notre 9ème Rapport d'activités 2001/2002, paragraphe 3.2.1.).

Le projet de loi prévoit également l'utilisation de données biométriques à des fins d'identification. Une liste exhaustive de ces données sera ancrée dans l'ordonnance d'application. En ce qui concerne les risques d'atteinte à la personnalité en raison de

l'utilisation de données biométriques, nous vous renvoyons au paragraphe 3.1.1 du présent rapport.

Le point le plus critique du projet de loi est l'utilisation de la vidéosurveillance ou de systèmes de reconnaissance (y compris par comparaison avec des systèmes de recherche) non seulement à des fins d'identification des personnes ne pouvant pas entrer sur le territoire suisse et devant être prises en charge par les compagnies aériennes les ayant transportées, mais également à d'autres finalités, telles que l'augmentation des mesures sécuritaires ou l'échange d'informations. En ce qui concerne la première finalité, le nombre de personnes visées étant très faible, se pose la question de la proportionnalité de la mesure envisagée. Quant aux autres finalités, nous sommes d'avis que l'utilisation de tels moyens pour accomplir des tâches légales non définies ne saurait être justifiée dans le cadre du présent projet de loi. Ces mesures doivent en effet d'une part s'inscrire dans un examen plus approfondi, prenant en particulier en compte l'équilibre entre les droits des individus et la mise en place de mesures de sécurité proportionnées, et être d'autre part élaborées, si leur nécessité est démontrée, dans le cadre de législations relevant de la police ou de la sécurité intérieure et non pas dans la loi sur les étrangers.

3.2.2 Dispositions de protection des données dans les accords de réadmission et de transit

Dans le cadre d'accords de réadmission et de transit avec des Etats ne disposant pas de législation en matière de protection des données, la communication d'indications sur la nature de la décision de renvoi ou sur l'autorité ayant rendu la décision ne respecte pas les principes de finalité et de proportionnalité. En effet, une telle communication ne constitue pas un moyen nécessaire et apte à atteindre le but recherché, à savoir informer les autorités requises que la personne à réadmettre ou en transit présente un risque concret et actuel pour sa propre sécurité et pour celle des autorités requises ou des agents d'escorte.

Nous avons été consultés ces derniers mois au sujet d'accords de réadmission et de transit entre la Confédération suisse et des Etats ne disposant pas d'une législation en matière de protection des données équivalente à la nôtre, notamment des Etats asiatiques et africains. Dans de tels cas, la protection des données doit être réglée expressément dans l'accord. Lors de la consultation des offices, nous avons jugé les dispositions de protection des données spécifiques conformes au droit suisse. Ces dispositions correspondent d'ailleurs dans une large mesure à celles déjà en vigueur. Une clause minimale de protection des données est annexée au présent rapport (voir

paragraphe 13.4). Nous avons cependant constaté que d'autres dispositions prévoyaient des traitements de données personnelles non conformes à la législation sur la protection des données. Il s'agit avant tout de la communication d'indications sur la nature de la décision (judiciaire ou administrative) de renvoi ou sur les autorités ayant rendu cette décision. Les projets d'accords et les rapports explicatifs ne mentionnaient généralement pas le ou les buts de la communication envisagée en violation du principe de finalité. Parfois il était mentionné que la communication aurait pour but d'indiquer aux autorités requises que la personne à réadmettre ou en transit présente un risque concret et actuel pour sa propre sécurité et pour celle des autorités requises ou des agents d'escorte. Nous estimons que la communication de la nature de la décision de renvoi ou de l'autorité ayant rendu la décision en question ne peut être un moyen nécessaire et apte pour assurer de manière optimale que les opérations au moment de la réadmission ou du transit se déroulent dans les meilleures conditions de sécurité. Une telle communication viole par conséquent le principe de proportionnalité. Par contre, la communication du fait que la personne concernée peut présenter un danger pour la sécurité publique, les autorités des deux pays (en particulier les escortes) ou elle-même constitue un moyen tout à fait adéquat pour atteindre le but recherché. Il faut également relever que les autorités requises, en se basant uniquement sur la nature de la décision de renvoi, pourraient tirer des conclusions totalement fausses sur la personne concernée.

3.2.3 Vidéosurveillance effectuée par les CFF dans la gare principale de Zurich

Le contrôle des installations de vidéosurveillance des CFF dans la gare de Zurich, que nous avions effectué en octobre 2001 déjà, a révélé des vices et eu pour conséquence que des améliorations ont été entreprises en ce qui concerne la protection des données. D'autre part, les bases légales nécessaires pour ces installations de vidéosurveillance des CFF vont être créées. Il reste néanmoins encore quelques questions non résolues.

Notre contrôle des installations de vidéosurveillance de la gare de Zurich (cf. notre 9ème rapport d'activités, paragraphe 3.2.2) a révélé que les diverses installations de vidéosurveillance avaient manifestement été mises en place sans que l'on ait disposé d'un concept clair. Même au sein des CFF, personne ne semblait vraiment avoir une vue d'ensemble de toutes les mesures de surveillance. Notre contrôle a soulevé ces problèmes et permis de sensibiliser les CFF à la problématique existante. C'est pourquoi des efforts ont été entrepris en vue de régler de manière claire la vidéosurveillance: d'une part, les CFF ont demandé au Conseil fédéral de créer une base légale,

d'autre part, ils ont mis sur pied un groupe de travail dont la tâche est de revoir les dispositions d'exécution existantes sur l'engagement de moyens de vidéosurveillance. Il est en outre prévu d'établir un registre de toutes les installations de vidéosurveillance des CFF afin d'être en mesure de répondre à temps et de manière compétente aux demandes internes et externes.

Les mesures déjà prises ainsi que les mesures prévues vont dans la bonne direction et doivent être poursuivies. Nous avons demandé à être informé sur l'état des travaux, notamment en ce qui concerne les points suivants:

- information sur la vidéosurveillance des personnes concernées;
- preuve de l'efficacité des installations pour permettre d'apprécier si le traitement des données est proportionnel;
- mise en place d'une séparation nette des responsabilités entre les CFF, la police cantonale zurichoise et Securitrans SA pour l'installation «Nœud Zurich»;
- suppression rigoureuse des enregistrements sur l'installation située dans le centre d'information et de vente des CFF après 24 heures, si aucun incident n'est survenu (procédure d'écrasement).

3.2.4 Groupe de travail sur la violence lors des manifestations sportives

Un groupe de travail interdépartemental a élaboré une série de mesures pour lutter contre la violence lors des manifestations sportives. Les mesures proposées portent gravement atteinte à la personnalité de l'individu. La mise en place de ce genre de mesures de sécurité nécessite donc la création de bases légales claires.

Nous participons à un groupe de travail interdépartemental sur la violence accompagnant les manifestations sportives. Placé sous la direction de l'OFSPO, ce groupe de travail est chargé de se prononcer entre autres sur le caractère licite et approprié de mesures destinées à empêcher les actes de violence et de vandalisme durant les manifestations sportives. Il s'agit de mesures telles que la surveillance par caméras vidéos, l'échange d'informations sur des hooligans, l'établissement d'un fichier de hooligans, l'interdiction d'accès aux stades dans toute la Suisse, etc. Ces mesures telles qu'elles sont proposées portant une atteinte considérable à la personnalité de l'individu, il convient de tenir compte de divers aspects relevant de la protection des données lors de cet examen.

Si ces mesures devaient être appliquées, une première source de problèmes serait le fait que divers organes traitent les données en question (autorités fédérales et canto-

nales, personnes privées ainsi que responsables de stades et associations de football), et que les lois sur la protection des données ne sont pas les mêmes pour tous les participants. Les organes de la Confédération et les personnes privées doivent respecter la LPD, les autorités cantonales (par exemple la police) doivent se conformer aux lois cantonales sur la protection des données. Toutes les lois sur la protection des données ont néanmoins en commun le fait qu'elles sont des lois-cadre qui ne posent que les principes d'un traitement licite des données. Les détails de la manière concrète dont les données seront traitées (par ex. la création d'un fichier de hooligans ou des dispositions pénales particulières concernant les hooligans) doivent être réglés dans des lois spéciales.

Dans l'état actuel des choses, le projet «Violence lors des manifestations sportives» contient trop de questions de principes encore en suspens. Mais nous pouvons au moins retenir une chose avec certitude: les bases légales actuelles ne permettent pas l'application immédiate des mesures proposées. Etant donné qu'en l'occurrence, des données personnelles particulièrement sensibles seraient touchées, la création d'une base légale formelle est indispensable. Ce n'est que lorsque nous connaîtrons les mesures concrètes que les autorités entendent prendre contre l'augmentation de la violence dans les stades qu'il sera possible de procéder à un examen détaillé sous l'angle du respect de la protection des données.

4. Informatique et télécommunication

4.1 La protection des données dans le domaine des télécommunications

Nous recevons quotidiennement plusieurs demandes concernant des questions de protection des données dans le domaine des télécommunications, soit de personnes concernées, soit de maîtres de fichiers. Nous avons rassemblé une partie des réponses aux questions les plus fréquentes et les publions continuellement sur notre site web. Vous trouverez également un extrait des questions et réponses dans l'annexe de ce rapport (voir paragraphe 13.2).

4.2 Clause minimale de protection des données dans les conditions générales des fournisseurs de services de télécommunication

Plusieurs fournisseurs de services de télécommunication (téléphonies fixe et mobile) ont modifié leurs conditions générales. Nous avons été consultés par les fournisseurs même ou par les clients au sujet de la validité des clauses relatives à la protection des données. Nous avons constaté que certaines clauses ne remplissaient pas les condi-

tions de la loi sur la protection des données, en particulier les principes généraux de finalité et de transparence ainsi que les normes afférentes à l'information et au consentement des personnes concernées. Il est en effet nécessaire d'informer les clients de la possibilité de s'opposer à un traitement de données, notamment à un traitement qui n'est pas nécessaire à la fourniture de prestations comme par exemple le traitement de données à des fins de marketing. Dans ce cadre, nous avons élaboré une clause minimale de protection des données que vous trouverez annexé au présent rapport (voir paragraphe 13.1).

4.3 Formules de réexpédition de la Poste et mise à jour des adresses – la décision du DETEC

Grâce à une décision prise par le DETEC en avril 2002, la pratique de la Poste concernant les formules de réexpédition que nous critiquions depuis plusieurs années a finalement pu être rendue conforme aux exigences de la protection des données. Suite à notre intervention, la Poste a fortement réduit la taxe pour les clients qui renoncent à la mise à jour des données. Elle a également corrigé certaines explications peu compréhensibles que contenaient les formulaires. Nous avions déjà demandé ceci dans notre recommandation.

Une formule de réexpédition doit être remplie par quiconque désirant que, suite à un changement de domicile, le courrier adressé à son ancienne adresse soit réexpédié à la nouvelle adresse. Une telle réexpédition est coûteuse, c'est pourquoi la Poste propose un service de mise à jour des adresses en collaboration avec l'entreprise DCL. Ce service permet aux entreprises de mettre à jour leur fichier d'adresses pour réduire ainsi le nombre d'envois mal adressés. Toute personne faisant une demande de réexpédition est cependant libre de refuser la mise à jour de son adresse auprès de tiers. Suite à nos interventions, la Poste avait accepté ce droit du client, mais avait dans ce cas exigé à partir de 2001 que le client paie une taxe se montant à 24 fois la taxe normale (calculé sur une année). Étant donné que cette pratique influençait fortement la liberté de décision des clients, nous avions émis le 19 février 2001 une recommandation demandant à la Poste d'exiger au maximum le double de la taxe usuelle dans les cas où le client refusait la mise à jour auprès de tiers. Nous avions également critiqué certaines explications peu claires que l'on trouvait sur la formule ainsi que sur la feuille explicative l'accompagnant et avions demandé qu'elles soient corrigées. La recommandation peut être consultée en ligne sous http://edsb.ch/d/doku/empfehlungen/postsendung_d.pdf. Étant donné que la Poste a rejeté notre recommandation, nous avons décidé le 27 avril 2001 de porter l'affaire pour décision

auprès du DETEC. Le 25 avril 2002, le département a statué sur notre recommandation (voir annexe, paragraphe 13.3) et a entièrement repris nos exigences (à l'exception de notre demande de remboursement des taxes déjà payées). La Poste a appliqué la décision du DETEC et exige depuis juin 2002 une taxe de 15 francs par année pour la réexpédition du courrier dans les cas où le client accepte la mise à jour des adresses auprès de tiers et 30 francs par année dans les cas où le client refuse cette mise à jour (comparé à 20 francs par mois précédemment!).

4.4 Révision de la loi sur les télécommunications et de la loi sur la radio et la télévision

Aussi bien la loi sur les télécommunications que la loi sur la radio et la télévision se trouvent actuellement en cours de révision. Dans le cadre des deux procédures de consultation des offices, nous avons dû constater que les dispositions respectives sur la protection des données ont été formulées de manière bien trop vague.

Nous avions été invités dans le cadre de la consultation des offices à prendre position sur la révision partielle prévue de la loi sur les télécommunications, de l'ordonnance sur les services de télécommunication ainsi que sur l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications. Du point de vue de la protection des données, nous étions surtout intéressés par les dispositions régissant les traitements de données ainsi que l'entraide administrative. La législation en matière de protection des données exige que les traitements de données effectués par des autorités fédérales reposent sur une base légale. Nous avons dû constater que ces articles relatifs aux traitements de données ont été formulés de manière bien trop imprécise et ne constituent donc pas une base légale suffisante. Nous avons demandé notamment que les catégories de données devant être traitées, les buts des traitements de données ainsi que les organes impliqués soient explicitement mentionnés dans le texte de la loi. Nous avons également demandé que les systèmes d'information, leurs buts ainsi que les accès à ces systèmes soient clairement décrits. En ce qui concerne l'entraide administrative, nous avons fait remarquer que celle-ci ne peut être accordée que dans des cas isolés et sur demande motivée. Nous avons donc proposé de renoncer à la fourniture de listes qui était prévue dans le cadre de l'entraide administrative. Nous avons également retenu que l'obligation d'annoncer prévue devait être précisée en ce qui concerne l'envergure des données à communiquer et les autorités impliquées. Finalement, nous avons salué le fait qu'il est prévu de régler l'envoi de courrier électronique non sollicité (spamming).

Peu de temps après, nous avons également été invités, dans le cadre de la consultation des offices, à prendre position sur la révision totale de la loi sur la radio et la télévision. Il est utile de relever le fait que cette révision totale prévoie également des modifications dans la loi sur les télécommunications, entre autres dans les dispositions susmentionnées. Cela signifie, en d'autres mots, que ces dispositions se trouvent dans les deux révisions. Dans notre prise de position concernant la révision de la loi sur la radio et la télévision, nous avions entre autres rendu attentif au fait que la disposition relative à la protection des données a été formulée de manière bien trop vague. Nous avons demandé que soient mentionnés au moins le but et l'ampleur des traitements de données, les organes impliqués ainsi que les catégories de données. En ce qui concerne les dispositions de la loi sur les télécommunications, nous avons réitéré dans les grandes lignes les remarques que nous avions déjà faites dans le cadre de la révision partielle de la loi sur les télécommunications.

Il en découle que les exigences de la protection des données n'ont pas suffisamment été prises en compte, notamment dans la loi sur les télécommunications.

5. Santé

5.1 Thèmes divers

5.1.1 Exigences techniques de base pour un dossier médical électronique du patient

Dans le cadre de l'électronisation du dossier médical du patient, nous avons cherché à formuler quelques exigences ou recommandations de base auxquelles cette évolution quasi inéluctable devrait satisfaire, quel que soit le modèle retenu (central, décentral, patient, carte…) pour la mémorisation physique de ce dossier. Il est fort probable que les nombreux projets et modèles en développement dans notre pays nous conduiront à réviser, adapter ou nuancer certains points de vue en fonction des expériences faites dans le domaine.

Pour préciser le contexte, il est important d'envisager les différents modèles possibles pour la localisation du dossier électronique du patient:

1. Décentralisé ou distribué, c'est-à-dire que les données médicales restent chez les prestataires de soins et qu'un dossier virtuel contenant la «partie publiée de chaque épisode» est reconstitué si nécessaire en faisant appel à un réseau fédérateur utilisé par tous les partenaires. La disponibilité intégrale d'un tel dossier virtuel est

évidemment une question clé, associée à l'éventuelle nécessité de centraliser malgré tout certaines données personnelles.

2. Centralisé chez un tiers, c'est-à-dire que tout ou partie des données médicales établies par un prestataire de soins est copiée dans un registre central géré par un organisme étatique (canton, Confédération) ou privé (fournisseur de services). La confiance envers l'organe centralisateur, de même que le point d'attaque qu'il représente, sont des problèmes inhérents à ce modèle.

3. Centralisé chez le patient lui-même, c'est-à-dire que tout ou partie des données médicales établies par un prestataire de soins est copiée sur un support (carte à puce, CD…) détenu par l'intéressé. La disponibilité des données resterait ainsi exclusivement sous le contrôle du patient, tandis qu'une copie de sauvegarde du support pourrait même être laissée en dépôt chez le médecin de confiance.

Ces trois modèles théoriques peuvent en pratique être combinés de différentes manières. La carte patient peut en particulier être envisagée comme simple objet d'identification (numéro d'assuré, nom…), comme support de mémorisation des données administratives et/ou d'urgence, comme clé cryptographique d'accès aux données médicales proprement dites, voire enfin comme support de mémorisation du dossier médical du patient.

Voici à ce stade qu'elles pourraient être les contraintes de protection des données à prendre en considération indépendamment du modèle de mémorisation choisi:

- Distinction entre données administratives et données médicales. Parmi les données médicales, distinction plus fine entre données objectives (examens…), données subjectives (diagnostics…), données de médication et données d'urgence. L'accès à ces dernières doit être réglé de manière spécifique, étant donné la criticité des cas d'urgence.

- Format de stockage et de codage de toutes les données assurant la pérennité et l'interopérabilité nationale voire internationale (saisie/conversion des données actuelles).

- Usage prépondérant des nouvelles technologies de pseudonymisation et d'anonymisation des données (cf. 9ème rapport d'activités, paragraphe 2.2.1) de manière à limiter au maximum les risques de fuite de données personnelles et à permettre au mieux l'exploitation épidémiologique ou statistique des données médicales récoltées.

- Mémorisation chiffrée des données personnelles sensibles: seules les personnes en possession de clés valides de déchiffrement sont à même de lire et/ou écrire des épisodes du dossier. Chaque épisode médical peut en effet faire l'objet d'un

chiffrement distinct, pour lequel le patient (éventuellement son médecin de confiance) devrait en principe posséder une clé de lecture. La réalisation d'un tel environnement de chiffrement présuppose le déploiement non trivial d'une infrastructure à clés publiques (PKI).

- Possible masquage provisoire des données médicales méritant une explication orale par le prestataire de soins spécialisé.
- Identification systématique et authentification forte de tous les acteurs de la santé ayant accès au système.
- Journalisation exhaustive et disponible en tout temps pour la personne concernée de tous les accès et de toutes les mutations de données sensibles.
- Garantie et revue périodique de confidentialité, intégrité et disponibilité des données.
- Signature numérique de toutes les données enregistrées, pour assurer leur non-répudiabilité et leur intégrité.
- Visibilité différenciée (vues logiques) des données assurée pour tous les ayants droit.
- Canal d'information spécifique et proportionnel avec les assurances qui reçoivent les éléments de facturation possiblement sous une forme chiffrée à convenir (cf. paragraphe 5.1.2 du présent rapport).
- Solution également spécifique pour les ordonnances et les accès par les pharmaciens.

5.1.2 Carte d'assuré et carte de santé

Le Conseil fédéral a décidé, dans le cadre de l'assurance-maladie obligatoire, d'introduire une carte d'assuré. La carte d'assuré sera obligatoire, munie d'un numéro d'identification et d'une interface «utilisateur» et sera utilisée pour la facturation électronique des prestations. Elle permettra en outre la mémorisation facultative d'autres informations (informations pour les cas d'urgence). Les risques liés à la protection des données d'une telle carte dépendent de son contenu, de l'emploi prévu et du domaine d'application.

Dans notre dernier rapport d'activités, nous avions défini les exigences minimales devant être respectées pour l'introduction d'une carte de santé (9ème rapport d'activités 2001/2002, paragraphe 5.1.1). Il n'était pas encore clair à l'époque si le but poursuivi était une carte d'assuré à des fins purement administratives ou une vraie carte

de santé. Cette dernière a été présentée comme une sorte de clé électronique qui permet d'accéder à toutes les données médicales d'une personne (dossier médical électronique). Les risques du point de vue de la protection des données sont différents pour les deux cartes. La carte d'assuré administrative peut être déclarée obligatoire, à condition que son contenu ainsi que les finalités de son utilisation soient clairement définis. Une carte de santé, qui contient des informations médicales ou permet même de consulter l'historique médical couvrant la vie entière du patient, est par contre bien plus délicate du point de vue de la protection des données. La possession ainsi que l'utilisation d'une telle carte doivent être facultatives. Le détenteur de la carte doit être le seul maître des données qui y sont mémorisées et pouvoir décider en toute liberté à qui, quand et dans quelle mesure il permet l'accès à ses données médicales. Un historique médical qui couvre la vie entière d'une personne est un fichier spécial qui, de par sa nature même, ne devrait pas contenir un minimum, mais plutôt un maximum de renseignements. Ceci ne pose aucun problème aussi longtemps que la sécurité des données est garantie et que l'accès à ces dernières reste réservé à la personne concernée ainsi qu'au personnel médical qu'elle y autorise. Mais il est très vraisemblable que très vite des tiers feront part de leur vif intérêt pour certaines des données contenues dans cette collection électronique d'informations médicales recueillies au cours de toute une vie. Il est prévisible qu'avec l'existence de tels dossiers médicaux sous forme électronique, la pression va augmenter envers les personnes à divulguer certaines informations concernant leur état de santé dans certaines conditions, par exemple lorsqu'elles sollicitent un emploi ou lorsqu'elles concluent une assurance.

En août 2002, le Conseil fédéral a décidé, dans une première étape, d'introduire une carte d'assuré dans le cadre de l'assurance-maladie obligatoire. Cette carte d'assuré doit répondre à deux objectifs: permettre d'une part l'identification univoque de l'assuré moyennant un numéro d'identification, d'autre part la facturation électronique des prestations fournies en vertu de la LAMal.

Comme numéro d'identification, on pourrait utiliser le nouveau numéro AVS (cf. paragraphe 6.1.3). Il est prévu de faire évoluer ce numéro pour qu'il devienne un vrai numéro d'assurance sociale. Il n'y a en principe aucune objection à cela, pour autant que ce numéro d'assurance sociale soit utilisé conformément aux dispositions prévues dans la loi, à savoir:

- qu'il ne peut être utilisé que pour les buts explicitement prévus dans la loi;
- qu'il ne peut être utilisé que dans le domaine des assurances sociales.

Si l'utilisation de numéros d'identification est délicate du point de vue de la protection des données, c'est parce qu'elle facilite grandement la mise en relation de don-

nées. Si le même numéro ou plusieurs numéros différents pouvant être mis en relation sont utilisés à des fins différentes dans des domaines différents, les données de ces différents domaines de la vie d'une personne peuvent être mises en relation et utilisées pour créer ce qu'on appelle un profil de la personnalité. C'est la raison pour laquelle l'utilisation de numéros d'identification doit être restreinte à des domaines définis et réglée de manière détaillée dans la loi. La preuve que ceci est nécessaire est donnée par les expériences faites avec l'actuel numéro AVS qui en pratique s'est très rapidement répandu de manière incontrôlée pour être aujourd'hui utilisé par un grand nombre d'organismes pour les usages les plus divers. Une telle utilisation non contrôlée du numéro d'assurance sociale doit être évitée dès le début, d'autant plus que les moyens modernes de communication électronique ont fortement augmenté et facilité les possibilités de mise en relation des données (cf. également paragraphe 6.1.3).

La carte d'assuré sera une «carte à interface utilisateur». Un mini-ordinateur permettra d'accéder aux données d'identification et de gérer les données personnelles de l'assuré qui sont enregistrées sur la carte. Une fois que la carte d'assuré aura été introduite, la facturation devra obligatoirement se faire par l'intermédiaire du système électronique (utilisant la carte d'assuré).

L'introduction de la facturation électronique est liée au projet TarMed, qui de son côté laisse encore un certain nombre de questions importantes en matière de protection des données sans réponse (cf. paragraphe 5.1.5). Les factures de prestations contiennent aujourd'hui déjà des informations détaillées concernant l'état de santé de la personne concernée. Une fois que le système TarMed aura été introduit, les factures seront encore plus détaillées. Ainsi les factures mentionneront à l'avenir le code de diagnostic CIM-10 très controversé. D'autre part, le fait que les données soient présentes sous forme électronique facilitera non seulement leur dépouillement, mais en augmentera les possibilités. C'est pourquoi nous sommes d'avis que les problèmes liés à la protection des données doivent être réglés avant que la facturation électronique ne soit introduite. Cela signifie selon nous que:

- le flux de données entre les fournisseurs de prestations et les assureurs doit être revu et limité à un volume de données approprié et minimal;
- le contrôle général des prestations et de leur caractère économique doit être effectué avec des données pseudonymisées, étant donné qu'il s'agit d'un contrôle des fournisseurs de prestations qui ne nécessite pas de données relatives au patient;
- le contrôle des prestations et de leur caractère économique dans les cas isolés doit être impérativement effectué par l'intermédiaire du médecin-conseil (ou le cas échéant d'un institut neutre à désigner);

- les données qui servent au contrôle des prestations et de leur caractère économique dans les cas isolés doivent être supprimées une fois que les contrôles ont été faits, étant donné qu'elles ont rempli leur fonction et que toute autre utilisation violerait le principe de la finalité;
- l'instrument du médecin-conseil, qui est actuellement engagé uniquement dans le domaine de l'assurance-maladie obligatoire, soit renforcé et étendu;
- une instance de contrôle indépendante garantisse que les données sensibles (informations médicales et diagnostics) restent auprès du médecin-conseil;
- l'on envisage la mise en œuvre d'instances d'audit et de certification indépendantes.

Lors de l'introduction de la facturation électronique, les problèmes existants dans le domaine de la facturation des prestations ne doivent pas simplement être repris, ils doivent être résolus de manière pratique et acceptable.

Que l'on opte pour une carte d'assuré obligatoire ou pour une carte de santé facultative, les systèmes de traitement des cartes doivent en tous les cas être configurés de manière à ce que les principes de base de la protection des données, à savoir la proportionnalité, la transparence et un traitement des données qui corresponde à la finalité soient respectés. La responsabilité que ces principes fondamentaux soient appliqués incombe aux organes qui introduisent ces systèmes. En ce qui concerne le système de facturation électronique, cela signifie que les assurés doivent être informés de manière claire et compréhensible sur les types de traitement qu'entraînera cette facturation. Ceci inclut également des réponses aux questions du genre: quelles sont les données minimales nécessaires pour établir le décompte? Quelles sont les données communiquées? Qui sont les destinataires? A quelles fins ces données sont-elles utilisées? Pour quelle durée sont-elles conservées? Quelles sont les mesures envisagées pour assurer la sécurité des données?

5.1.3 Enquêtes effectuées par des instituts auprès d'assurés

Au cas où des tiers seraient engagés pour effectuer des enquêtes facultatives, la communication des données nécessaire à l'exécution des enquêtes doit se faire dans le respect du principe de la proportionnalité. Cela signifie que seules les données qui sont vraiment nécessaires pour l'exécution de l'enquête peuvent être communiquées. Cela présuppose que le mandant doit tout d'abord déterminer qui participera à l'enquête. La communication du fichier d'adresses intégral est disproportionnée.

Dans la pratique, l'exécution d'enquêtes est de plus en plus souvent confiée à des instituts externes. C'est ainsi qu'une compagnie d'assurance a mandaté l'année passée un institut pour effectuer un sondage auprès de ses assurés. Elle communiqua à cette fin à l'institut les adresses d'un grand nombre de ses assurés avec mention du nom du médecin traitant.

Un grand nombre de ces assurés ont été surpris et étonnés de recevoir du courrier d'un institut qu'ils ne connaissaient pas et qui contenait une information sensible, à savoir le nom de leur médecin traitant. Pour cette raison, ils se sont plaints auprès de nous.

Les principes généraux, applicables à la communication de données, stipulés dans la loi sur la protection des données – tels que le principe de la bonne foi, de proportionnalité, de finalité – sont toujours valables, même si le mandat est confié à un tiers, ce qui est en soi permis. La participation à une enquête est en règle générale facultative. L'assuré sélectionné doit donc avoir la possibilité – avant que ses données soient communiquées à un tiers – de refuser de participer et d'interdire ainsi la communication des données le concernant. Cela signifie que la compagnie d'assurance aurait dû contacter les assurés sélectionnés avant de communiquer les données à l'institut pour leur demander s'ils étaient d'accord de participer à l'enquête et s'ils consentaient à la communication des données nécessaires à l'enquête. Il s'agissait dans le cas précis non seulement de l'adresse de l'assuré, mais également d'une information sensible, à savoir le nom du médecin traitant qui pouvait éventuellement permettre de tirer certaines conclusions, notamment dans les cas où il s'agissait d'un médecin spécialiste tel qu'un oncologue ou un psychiatre. Il est d'autre part bien entendu que le caractère facultatif de l'enquête devait explicitement être mentionné autant sur la demande de consentement que sur le questionnaire même. Si la compagnie d'assurance avait procédé de la manière décrite, l'institut n'aurait reçu que les données des assurés qui étaient prêts à participer à l'enquête. Ils auraient également été les seuls à recevoir du courrier.

Il existe pourtant une méthode simple de demander le consentement des personnes concernées pour une telle enquête et de respecter ainsi le principe de la proportionnalité: la compagnie d'assurance envoie elle-même le questionnaire aux assurés, les informe en même temps de manière détaillée sur l'objectif de l'enquête ainsi que sur la démarche et leur demande de renvoyer le questionnaire directement à l'institut qui procédera alors au dépouillement anonyme des données.

5.1.4 Manque de transparence et collecte disproportionnée de données dans le système RAI/RUG

Des organisations d'aînés se sont adressées à l'association des Commissaires suisses à la protection des données pour lui demander d'apprécier le système RAI/RUG du point de vue de la protection des données.

Le système RAI/RUG est utilisé dans plusieurs cantons pour le recensement systématique du besoin de soins des résidents de homes en vue de les classifier en fonction de leur charge de soins. Au sein de l'association des Commissaires suisses à la protection des données, c'est le groupe de travail «Santé» (AGX) qui a été chargé d'étudier cet outil d'appréciation. Il conclut dans son rapport que le système est en grande partie opaque pour les résidents des homes. Outre ce manque de transparence, l'AGX constate que le nombre de données recueillies et enregistrées de manière systématique est bien trop élevé et donc non conforme au principe de la proportionnalité.

Vous trouverez le rapport détaillé du groupe de travail AGX ainsi qu'une liste des adaptations nécessaires à l'adresse http://www.dsb-cpd.ch/f/publikationen/rapport-rai-rug.htm. Ces documents sont également inclus dans les annexes de ce rapport d'activités (paragraphe 13.5).

5.1.5 Le tarif médical TarMed

Au cours des dernières années, nous avons à plusieurs reprises rendu attentif les responsables du projet TarMed à des questions délicates en matière de protection des données. Entre-temps la date d'introduction de TarMed a été fixée. Malgré cela, nous n'avons toujours pas été officiellement informés sur la nature du système qui a été choisi ainsi que sur les mesures de protection et de sécurité des données. Il ne nous est donc pas possible de juger si les questions relevant de la protection des données ont été résolues de manière satisfaisante. Cela signifie que – du point de vue de la protection des données – nous ne sommes toujours pas en mesure de clore ce dossier.

Le tarif médical TarMed entrera en vigueur le 1er mai 2003 pour les assurances accident, militaire et invalidité et le 1er janvier 2004 pour l'assurance-maladie. Ce nouveau système tarifaire crée une structure uniforme des tarifs pour l'ensemble de la Suisse. Les conventions passées entre les partenaires tarifaires (FMH, santésuisse, H+) stipulent que les dispositions légales de la protection des données doivent être respectées. L'application pratique de ces dispositions et, ce faisant, des mesures concrètes de protection des données est de la responsabilité des parties qui introduisent le système.

Nous nous efforçons depuis des années à faire accepter que les droits de la personnalité des assurés soient respectés lors de l'introduction de TarMed. Bien que l'introduction soit imminente, les responsables du projet ne nous ont – malgré plusieurs rappels – toujours pas informés sur ce qui est concrètement prévu. Il nous est ainsi impossible de procéder à une appréciation des aspects liés à la protection des données avant de savoir quelles sont les mesures concrètes qui ont été prises.

Les questions relevant de la protection des données n'ont toujours pas été résolues. Les deux principaux points controversés sont d'une part l'indication sur les factures des codes détaillés de diagnostic et d'interventions chirurgicales (CIM-10 et CHOP), d'autre part la facturation électronique des prestations qui deviendra obligatoire avec l'introduction de TarMed et de la carte d'assuré (cf. paragraphe 5.1.2 du présent rapport).

Nous avons déjà exposé notre position à plusieurs reprises lors d'entrevues avec les parties impliquées dans le projet TarMed. Nous avons également publié notre point de vue dans plusieurs de nos rapports d'activités (cf. 9ème rapport d'activités 2001/2001, paragraphe 5.1.4; 8ème rapport d'activités 2000/2001, chapitre I.7.5; 6ème rapport d'activités 1998/1999, chapitre I.8.3). Voici encore une fois nos principales constatations:

- La communication systématique aux assureurs de diagnostic, de codes de diagnostic ou d'autres codes compatibles est non seulement contraire au principe de proportionnalité ancré dans la loi sur la protection des données mais viole également l'article 42 LAMal. Le principe de la proportionnalité ne permet de récolter que les données vraiment nécessaires et appropriées pour le but poursuivi; c'est surtout en présence de données sensibles qu'une importance accrue doit être donnée au respect de ce principe. Le principe de la proportionnalité s'applique également à la collecte de données effectuée en vertu de l'article 42 LAMal. La seule communication systématique autorisée est donc celle du «diagnostic sommaire», à savoir d'un diagnostic général tel qu'il est requis pour un cas normal moyen.

- S'il devait s'avérer, dans des cas isolés motivés, que ce «diagnostic sommaire» ne devait pas suffire, l'assureur peut par la suite demander un diagnostic plus détaillé ou des informations médicales complémentaires. Du point de vue de la protection des données, ces informations complémentaires doivent impérativement être obtenues par l'intermédiaire du médecin-conseil de l'assureur. L'article 42 alinéa 5 LAMal prévoit néanmoins que l'assuré peut exiger que ces informations complémentaires soient communiquées uniquement au médecin-conseil. Elle prévoit cependant qu'il prend lui-même l'initiative, ce qui n'est pas satisfaisant du point de vue de la protection des données.

- Le principe de transparence exige que les besoins en données ainsi que les procédés de traitement de données liés à la facturation – indépendamment du fait que celle-ci se fasse de manière électronique ou non – soient communiqués à l'assuré de manière claire et compréhensible.
- Le système de facturation électronique doit mettre en œuvre les technologies respectueuses de la protection des données qui sont aujourd'hui disponibles: procédés d'anonymisation et de pseudonymisation, procédés de chiffrement, signature numérique, etc.
- La sécurité des données doit être assurée en utilisant les technologies les plus modernes en la matière.

Il n'est pas dans l'intention de la protection des données d'empêcher la facturation électronique, ni les contrôles nécessaires et absolument incontestés de cette dernière. Les systèmes prévus doivent cependant prendre en compte les aspects de protection des données en étant configurés de manière à traiter un minimum de données, en respectant les principes de la protection des données et en permettant à l'assureur d'effectuer ses contrôles de manière à ce que le secret médical soit respecté. Ceci est possible par ex. en utilisant des procédés de pseudonymisation. Quant au contrôle du caractère économique des fournisseurs de prestations, il suffit de procéder à un examen général sur la base de données pseudonymisées. L'examen du caractère économique spécifique à l'assuré dans un cas isolé doit également être possible, mais il devrait à notre avis être effectué par le médecin-conseil ou un autre organe neutre.

5.2 Génétique

5.2.1 La protection des données interdit les tests de paternité subreptices

Les entreprises qui désirent commercialiser des tests de paternité en Suisse doivent prendre des précautions pour garantir qu'elles ont obtenu le consentement écrit de toutes les personnes concernées. Elles sont tenues de vérifier la validité des consentements écrits selon une procédure rigoureuse. Ce n'est qu'ainsi que l'on peut éviter que des prélèvements de tissu soient effectués à la dérobée sur des enfants dans le but d'exécuter des tests de paternité à l'insu du partenaire.

L'année passée, des entreprises privées ont commencé à proposer sur le marché suisse des tests de paternité extrajudiciaires. Pour l'instant, l'exécution de tels tests

ne nécessite aucune autorisation et n'est soumise à aucune restriction de la part des autorités. Une réglementation légale n'existera qu'une fois que la future loi fédérale sur l'analyse génétique humaine (LAGH) sera entrée en vigueur.

La manière dont les tests de paternité sont proposés n'est pas conforme aux prescriptions de la protection des données. L'exécution d'un test de paternité constitue un traitement de données personnelles au sens de la loi sur la protection des données. Dans la mesure où un tel test n'a pas été ordonné par un tribunal, il ne peut être exécuté que si les personnes concernées ont donné leur consentement écrit. Si les entreprises qui proposent des tests de paternité ne vérifient pas que les signatures nécessaires aient été fournies et que celles-ci proviennent effectivement des personnes concernées, il est sans autre possible de faire exécuter des tests de paternité à l'insu des personnes concernées. Les tests effectués à l'insu du partenaire et de l'enfant ne constituent non seulement une violation des droits de la personnalité de l'enfant concerné, mais également du partenaire à l'insu duquel le test est effectué.

Entre octobre 2002 et janvier 2003, nous avons adressé des recommandations à trois entreprises (voir paragraphe 13.7.2). Nous y avons invité les entreprises concernées à respecter les prescriptions de la loi sur la protection des données lors de l'exécution de ces tests de paternité et à procéder à une vérification efficace de la validité des consentements écrits présentés par la personne demandant le test. Les entreprises doivent en particulier vérifier que les enfants disposent du consentement de leur représentant légal. Cela présuppose en règle générale que les deux parents doivent donner leur consentement écrit pour le test. Pour que le consentement soit juridiquement valable, il faut également que les personnes concernées soient conscientes de la portée du test. Dans ce domaine, un devoir d'information spécial incombe aux entreprises commercialisant ces tests. Ils doivent informer et conseiller leurs clients de manière professionnelle. Etant donné que les tests de paternité touchent à des données personnelles sensibles, il va de soi que des mesures efficaces doivent être prises pour assurer la sécurité des données.

5.2.2 Loi fédérale sur l'analyse génétique humaine

En septembre 2002, le Conseil fédéral a approuvé le message relatif à la loi fédérale sur l'analyse génétique humaine. Le projet sera donc soumis au Parlement.

Au terme de maintes procédures de consultation, la loi sur l'analyse génétique humaine (LAGH) et le message y relatif sont désormais disponibles (pour plus de détails, voir FF 2002 VII 6841). La LAGH a pour objectif de protéger la dignité humaine, d'empêcher les abus et de garantir la qualité des analyses. Reste à savoir si une discrimina-

tion sur la base du patrimoine héréditaire peut effectivement être évitée grâce à cette loi; de trop nombreux points dans ce domaine extrêmement sensible restent encore à éclaircir. Quant aux exigences générales auxquelles doivent répondre les analyses génétiques, il convient de se reporter au dernier rapport d'activités (voir 9ème Rapport 2001/2002, paragraphe 5.2.1).

Le domaine d'application du projet de loi englobe les analyses génétiques dans le secteur médical, dans le domaine du travail, des assurances et de la responsabilité civile. Par ailleurs, cette loi réglementera l'établissement de profils d'ADN pour la détermination de la filiation ou pour l'identification de personnes. Il convient de saluer le fait que le champ d'application de la LAGH – contrairement à de précédents projets – sera régi de manière exhaustive. Le traitement des données génétiques, qui sont des données sensibles, nécessite une base légale claire et exhaustive. Les futures analyses génétiques correspondant à de nouveaux besoins ne seront possibles que si la loi est adaptée en conséquence.

Les analyses génétiques présymptomatiques sont fondamentalement interdites dans le domaine du travail, de l'assurance et de la responsabilité civile (ce sont des analyses dont le but est de déterminer les prédispositions à certaines maladies avant l'apparition des symptômes cliniques). Des exceptions sont néanmoins prévues à certaines conditions. Nul ne peut donc dire si la loi permettra d'éviter la discrimination de personnes possédant un «mauvais» patrimoine héréditaire. On peut en effet imaginer que dans le domaine du travail notamment, les exceptions prévues défavorisent certains collaborateurs ou même des groupes de population possédant certaines caractéristiques génétiques (pour plus de détails à ce propos, voir paragraphe 7.6).

La LAGH règle également les conditions auxquelles les profils d'ADN peuvent être autorisés pour établir la filiation hors procédure. En font également partie les tests de paternité que divers laboratoires offrent aujourd'hui déjà sur le marché (voir également paragraphe 5.2.1). Les tests de paternité entre autres ne devront être possibles que si les personnes concernées aient donné leur consentement écrit; le projet de loi prévoit cependant qu'un enfant incapable de discernement ne peut être représenté par la personne pressentie pour la détermination de sa filiation.

La loi fédérale sur l'analyse génétique humaine devrait être soumise au Parlement dans un avenir proche.

6. Assurances

6.1 Assurances sociales

6.1.1 Devoir d'information du fournisseur de prestations selon la LAA

Les fournisseurs de prestations (médecins et hôpitaux) doivent fournir aux assurances-accidents les indications nécessaires aux buts prévus dans la LAA. Les assurances-accidents persistent toutefois à requérir un devoir d'information total et systématique. Cette situation n'est pas sans poser de fréquents problèmes dans la pratique quant à la protection des données.

Selon la loi fédérale sur l'assurance-accidents (LAA), le fournisseur de prestations doit remettre à l'assureur une facture détaillée et compréhensible. Il doit également lui transmettre toutes les indications nécessaires pour qu'il puisse se prononcer sur le droit aux prestations et vérifier le calcul de la rémunération ainsi que le caractère économique de la prestation. Le devoir d'information est réglé de manière explicite à l'article 54a LAA (en vigueur depuis le 1er janvier 2001).

De l'avis des assurances, selon le principe des prestations en nature en vigueur dans le cadre de l'assurance-accidents obligatoire, les fournisseurs de prestations agissent sur mandat des assurances-accidents. Elles estiment par ailleurs que les assurances doivent examiner d'office l'état de fait (principe de l'examen d'office) et que les indications nécessaires doivent donc être comprises au sens de «complètes». Par ailleurs, les assurances critiquent l'aide-mémoire des Commissaires suisses à la protection des données relatif au rapport de sortie et d'opération et l'estime inapplicable au domaine couvert par la LAA. Cet aide-mémoire établit des critères précisant quelles informations concernant les sorties d'hôpital et les opérations peuvent être transmises aux assurances et quand elles peuvent l'être (pour plus de détails, voir le 9ème Rapport d'activités 2001/2002, paragraphe 6.1.3). Les assurances persistent néanmoins à demander aux hôpitaux, quel que soit le cas, des rapports complets de sortie et d'opérations.

Du point de vue de la protection des données, les problèmes proviennent surtout du fait que les assurances accordent trop peu d'attention au principe de la proportionnalité. Ainsi, elles demandent souvent de volumineux dossiers de patients ou de volumineux rapports d'opération ou de sortie. Les hôpitaux leur reprochent en outre de demander systématiquement des rapports complets. Conformément au principe de la proportionnalité, il conviendrait néanmoins d'examiner dans chaque cas – en partant du but poursuivi – quelles sont les données nécessaires et appropriées. La trans-

mission systématique de rapports aux assurances-accidents – quel que soit le but poursuivi – n'est compatible ni avec le principe de la proportionnalité, ni avec le secret professionnel selon l'article 321 CP. La collecte de données à titre préventif doit aussi être systématiquement évitée.

Les rapports de sortie contiennent surtout des informations destinées au médecin qui suivra ultérieurement le patient. Ces informations n'ont pas été rassemblées en vue de la déclaration de prestations. Si l'assurance désire avant tout être mesure de contrôler le caractère économique de la prestation, elle ne doit pas nécessairement connaître les noms des assurés. Une pseudonymisation maximale des données des assurés – telle qu'elle est actuellement à l'étude dans le domaine de l'assurance-maladie – doit être visée. En effet, le principe de la proportionnalité est expressément mentionné à l'article 54a LAA. Il implique aussi que les besoins de données des assurances soient fondés; il ne suffit pas que les assurances mentionnent que les rapports sont «nécessaires à l'établissement complet des dossiers».

Des entretiens sont actuellement en cours avec les milieux concernés pour permettre de trouver une solution. Nous estimons néanmoins indispensable une plus grande transparence dans les processus d'information au niveau des hôpitaux, des cabinets médicaux et des assurances entre autres. C'est le seul moyen de contrôler ces processus quant à leur conformité avec les principes de la protection des données et de les adapter à la législation en la matière. Les Commissaires suisses à la protection des données ont donc demandé aux assurances-accidents de préciser concrètement leurs besoins en matière de données, notamment de mettre au point des standards correspondants. Il convient en particulier de définir quelles données peuvent être demandées aux hôpitaux et dans quel but.

6.1.2 Lacunes en matière de réglementation dans le domaine la protection des données médicales

Le Conseil fédéral et nous-mêmes avons été invités dans un postulat à rédiger un rapport sur les lacunes en matière de réglementation dans le domaine de la protection des données médicales. Ce rapport doit porter sur l'ensemble du secteur des assurances sociales. Il sera publié au cours de l'année 2003 et fera l'objet d'une procédure de consultation auprès des milieux intéressés.

La Commission des affaires juridiques du Conseil national a invité le Conseil fédéral et nous-mêmes à élaborer un rapport complet sur la protection des données médicales dans l'ensemble du domaine des assurances sociales (cf. également le postulat 00.3178). Le rapport ne doit pas seulement mettre en lumière les lacunes en matière

de réglementation existant actuellement, mais examiner également l'évolution technologique du traitement électronique des données (pour plus de détails, voir le 9ème Rapport d'activités 2001/2002, paragraphe 6.1.1).

L'Institut du droit de la santé de l'Université de Neuchâtel a été mandaté pour effectuer ces travaux, lesquels ont avancé conformément aux plans. Il a notamment remis aux assurances sociales, en Suisse alémanique et en Suisse romande, un questionnaire complet. Le but de ce questionnaire était entre autres de promouvoir la transparence des processus d'information. Cette enquête a été accompagnée d'entretiens. Par ailleurs, la collaboration d'informaticiens spécialisés a été requise pour le domaine de l'informatique médicale. Des enquêtes ont également été menées auprès d'institutions étrangères; elles ont permis d'intégrer à cette étude des éléments de droit comparé. La publication des résultats du rapport est prévue au cours de l'année 2003. Parallèlement, des propositions de modification seront mises en consultation auprès des milieux intéressés, cela dans l'optique de l'élaboration du rapport du Conseil fédéral.

6.1.3 Le nouveau numéro AVS

Le numéro AVS sera remplacé par un nouveau numéro d'assuré. Contrairement à l'actuel numéro AVS, ce nouveau numéro ne permettra plus de déduire certaines indications sur la personne en question. Par contre, il sera appliqué dans l'ensemble du domaine des assurances sociales.

Le numéro AVS utilisé actuellement est un numéro d'identification «parlant» car il donne des indications sur la nationalité, le sexe, la date de naissance et dans une mesure limitée sur le nom. Le numéro AVS est obligatoire pour les assurances sociales AVS (Assurance vieillesse et survivants), AI (Assurance invalidité) ainsi que pour les APG (régime des allocations pour perte de gain). Par ailleurs, les administrations et autres institutions peuvent utiliser les numéros AVS à leurs propres fins.

Pour diverses raisons, il est prévu depuis plusieurs années déjà de remplacer l'actuel numéro AVS par un numéro «non parlant». Du point de vue de la protection des données, il n'est pas satisfaisant que le numéro AVS actuel permette d'identifier une personne jusqu'à un certain point. Contrairement à l'actuel numéro AVS, le nouveau numéro sera utilisé toute la vie durant.

L'Office fédéral des assurances sociales (OFAS) nous a dernièrement soumis une ébauche de projet portant sur un nouveau numéro d'assurance sociale «non parlant». En outre, le nouveau numéro sera utilisé comme numéro d'assurance sociale dans l'ensemble du domaine des assurances sociales. Le numéro pourrait notamment être utilisé pour la carte d'assuré prévue par la LAMal (voir paragraphe 5.1.2).

Du point de vue de la protection des données, il convient de se féliciter que le nouveau numéro d'assuré ne permette plus de déduire certaines indications sur la personne concernée. Nous ne prenons donc pas fondamentalement position contre l'introduction d'un numéro d'assurance sociale. Néanmoins, nous avons prié l'OFAS d'examiner si d'autres numéros pouvaient être utilisés de manière sectorielle dans certaines assurances sociales après avoir généré le numéro d'assurance sociale. La technologie actuelle devrait le permettre aisément. L'utilisation des numéros d'assurance sociale en dehors du domaine des assurances sociales (autorités fiscales, banques, associations, etc.) – c'est actuellement le cas avec le numéro AVS – doit en tout cas être prohibé. Au cas où les nouveaux numéros d'assurance sociale viendraient à être aussi utilisés dans d'autres domaines, les possibilités de connexion pourraient permettre la constitution d'une image complète de la personnalité ou même d'un profil de la personnalité. Il faut empêcher que le but initial de ce numéro d'assurance sociale soit détourné. L'utilisation du numéro d'assurance sociale doit donc se limiter à la législation sur les assurances sociales. Il convient en outre de prévoir une base légale claire réglementant le traitement des numéros d'assurance sociale. Enfin, nous avons demandé à l'OFAS d'élaborer un règlement de traitement.

Nous continuerons dans la mesure de nos possibilités à suivre l'évolution du projet et à en contrôler la compatibilité avec la protection des données.

6.2 Assurances privées

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

Au cours de l'année écoulée, nous nous sommes à nouveau penchés sur les conditions dans lesquelles une assurance-responsabilité civile est en droit de collecter des données personnelles. Les milieux concernés ont été invités à s'exprimer sur la question. Nous œuvrons actuellement à la mise au point de standards minimaux applicables à la collecte de données par les assurances-responsabilité civile.

Les assurances-responsabilité civile demandent à des psychiatres, à des biomécaniciens et autres spécialistes des expertises sur les personnes lésées, parfois sans le consentement de celles-ci. En outre, les personnes lésées ne sont pas toujours informées. Cette situation n'est pas sans poser un certain nombre de problèmes dans la pratique, notamment dans les cas de traumatismes de la nuque et de la colonne vertébrale (mécanismes de whiplash). Nous avons donc convié les milieux concernés

(assurances, avocats des personnes lésées et experts) afin d'avoir une image plus précise des divers points de vue.

A notre avis, une expertise ne peut être requise par l'assurance-responsabilité civile que si la personne lésée a donné son consentement. Conformément au droit à l'autodétermination individuelle en matière d'information, la personne lésée décide en premier lieu elle-même de ce qu'il advient des données la concernant; tant que le consentement est possible, ce motif justificatif a fondamentalement la priorité sur d'autres motifs justificatifs (pour plus de détails, voir le 9ème Rapport d'activités, paragraphe 6.2.2). Par ailleurs, l'Office fédéral de la justice (OFJ) a rendu un avis sur la question en droit pénal. L'avis de droit de l'OFJ établit que les expertises psychiatriques contenant des éléments nouveaux sont soumises au secret professionnel conformément à l'article 321 CP. Toujours selon l'OFJ, la remise de ces expertises aux assurances-responsabilité civile n'est donc possible qu'avec le consentement du lésé. Par contre, la transmission d'expertises anonymisées est autorisée dans tous les cas.

Les représentants des assurances sont d'avis que les assurances-responsabilité civile peuvent demander des expertises sans requérir le consentement de la personne lésée. Ils estiment notamment que ces expertises sont indispensables pour éviter les cas d'escroquerie à l'assurance et protéger l'ensemble des assurés. En outre, les expertises devraient être établies le plus vite possible car le facteur temps joue un rôle important. De leur point de vue, le motif justificatif de l'intérêt privé prépondérant est ainsi donné.

Les avocats des lésés insistent pour que les assurances-responsabilité civile ne puissent demander d'expertise sur les personnes lésées qu'avec le consentement de celles-ci. Des données sensibles sont traitées à cette occasion et ils estiment que le seul motif justificatif est le consentement de la personne lésée. Par ailleurs, ils précisent que celles-ci ont aussi un droit de participation qu'il convient de respecter. Enfin, ils sont d'avis que ce sont les personnes lésées et non les assurances-responsabilité civile qui doivent prouver les prétentions.

Du point de vue des experts, il est important de savoir dans quelles conditions légales ils peuvent établir leurs expertises; ils estiment qu'il n'est pas de leur devoir de vérifier s'ils agissent légalement ou pas; pour eux, un point particulièrement confus est celui de savoir si et auprès de qui un consentement doit être recueilli. La situation actuelle leur semble surtout confuse parce qu'ils sont menacés dans certains cas de faire l'objet d'une plainte pénale.

Malgré ces divergences d'avis, toutes les parties présentes ont admis qu'il convient d'améliorer la transparence de la collecte de données dans l'intérêt des personnes lésées.

Nous travaillons actuellement à la mise au point de standards minimaux applicables à la collecte de données personnelles par les assurances-responsabilité civile.

6.2.2 Le rôle du service médical des assurances privées

Des entretiens sont en cours entre la Fédération des médecins suisses (FMH) et l'Association suisse d'assurances (ASA) à propos de la protection des données. Le rôle du service médical des assurances privées constitue l'un des objets de ces discussions.

Mis à part dans la loi sur l'assurance maladie (LAMal), la fonction du médecin-conseil n'est réglementée dans aucun texte légal. Selon la LAMal, le médecin-conseil est indépendant vis-à-vis de l'administration de l'assurance; en outre, il fait en quelque sorte office de «filtre». En particulier, des données médicales sont transmises directement au médecin-conseil (et non à l'administration de la caisse) lorsque l'assuré le souhaite. Cette méthode respecte les droits de la personnalité des assurés et répond au principe de la proportionnalité tel que le requiert la protection des données.

La question se pose donc de savoir si d'autres assurances ne pouvaient également pas adopter le système du médecin-conseil. Depuis longtemps déjà, nous demandons que les services médicaux actuels (médecins d'arrondissement, services médicaux, etc.) des autres assurances soient aussi mis en oeuvre ou si nécessaire qu'ils soient introduits dans cet esprit (pour plus de détails, voir le 8ème Rapport d'activités, chapitre 6.4). Même si à l'exception de la LAMal, il n'existe pas de normes légales applicables aux services médicaux des assurances, il convient de respecter les principes de la protection des données. Cela vaut tout particulièrement pour les données sensibles telles les données relatives à la santé.

En effet, les services médicaux ne sont en soi pas une nouveauté dans le domaine des assurances privées. Nous renvoyons à ce propos à une recommandation élaborée par le milieu des assureurs et la FMH en 1986. Conformément à cette recommandation, des données médicales peuvent être adressées au service médical de la compagnie d'assurance et être conservées uniquement auprès de celui-ci.

Le rôle du service médical dans le domaine de l'assurance privée est également l'un des thèmes analysés actuellement par la FMH et l'ASA. Cette analyse sera également l'occasion de vérifier que le flux de données demeure conforme à la protection des données dans l'assurance-accidents obligatoire gérée par les assurances privées. Les discussions portent par exemple sur le fait de savoir si les informations très sensibles doivent tout d'abord parvenir au service médical et non directement au service administratif de l'assurance. Des données extrêmement personnelles comme le sida,

un diagnostic psychiatrique ou une toxicomanie par exemple peuvent entraîner les assurances sur le chemin de la stigmatisation ou de la discrimination. Le traitement doit donc – dans toute la mesure du possible – être limité au strict minimum (principe voulant que l'on fasse un usage restreint des données et que l'on en évite la collecte).

Nous saluons l'initiative de la FMH et de l'ASA car nous estimons nécessaire de contrôler l'ensemble du secteur des assurances privées dans l'optique de la conformité avec les principes de la protection des données. Il convient néanmoins d'attendre que des solutions acceptables et surtout conformes à la protection des données soient trouvées et appliquées à l'ensemble des assurances privées.

7. Secteur du travail

7.1 Communication d'informations par le médecin-conseil d'une entreprise

Lors d'absences pour cause de maladie ou d'accident, l'employeur peut demander à ce que l'employé soit examiné par le médecin-conseil de l'entreprise. Dans son activité médicale, le médecin-conseil est soumis au secret médical. Cette obligation vaut également envers l'employeur. Le médecin ne peut communiquer à l'employeur que ses conclusions médicales.

Pendant la durée des rapports de travail, l'employeur est autorisé à traiter les données de ses employés dont il a besoin pour l'exécution du contrat de travail. Lors d'absences pour cause de maladie ou d'accident, l'employeur est autorisé à faire examiner l'employé par le médecin-conseil de l'entreprise. Dans son activité médicale, le médecin-conseil est soumis au secret professionnel, appelé dans ce cas secret médical. Ce secret doit également être respecté vis-à-vis de l'employeur. Le médecin-conseil n'est autorisé à communiquer à l'employeur que ses conclusions d'ordre médical et ce uniquement dans la mesure où celles-ci sont nécessaires pour l'exécution du contrat de travail. En règle générale, il s'agit de constatations relatives à l'aptitude ou l'inaptitude au travail de l'employé, à son degré d'aptitude au travail (à plein temps, à temps partiel, pas du tout), à la cause de l'inaptitude au travail (maladie ou accident), à la durée probable de l'inaptitude ou d'autres observations du même genre. De telles informations sont nécessaires pour l'exécution correcte des rapports de travail, étant donné que l'employeur doit par exemple pouvoir organiser un remplacement en cas d'absence prolongée. Le médecin-conseil n'est par contre pas autorisé à communiquer des informations médicales sans le consentement de l'employé. Ceci vaut en particulier pour la communication de diagnostics.

7.2 Programmes d'espionnage du point de vue de la protection des données

Outre l'enregistrement de tous les courriels entrants et sortants, les programmes d'espionnage permettent également de relever tous les contenus d'écran ainsi que l'ensemble des touches actionnées sur le clavier et les séances de surf sur Internet. Les employeurs qui utilisent ce moyen pour contrôler leurs employés contreviennent aux dispositions légales de protection des données et sont de ce fait punissables.

Dans la plupart des cas, les programmes de surveillance sont mis en place sans que la personne concernée en soit informée et permettent un contrôle permanent et précis de toutes les activités de l'employé à son poste de travail électronique. Grâce à eux, il est notamment possible de consulter les courriels: ceux-ci sont enregistrés et transmis à une adresse tierce. La «photographie» ou la «copie» de l'écran avec l'ensemble de son contenu (par ex. les pages Internet) à intervalles réguliers (recurrent screenshots) font aussi partie des fonctions des programmes d'espionnage. Par ailleurs, ces programmes peuvent saisir l'ensemble des touches actionnées sur le clavier, enregistrer les mots de passe introduits, indiquer toutes les applications actives, consulter le disque dur de l'ordinateur personnel, écouter les fichiers audios passés sur l'ordinateur, etc. Les programmes de surveillance permettent aussi la sauvegarde des enregistrements et des informations recueillis. Il est possible que le traitement de ces données aille encore plus loin, par exemple sous forme de communication des données à des tiers. Ce sont donc des systèmes performants grâce auxquels il est possible de surveiller en secret le comportement des employés sur le lieu de travail. De ce fait, ils constituent une violation de l'interdiction de surveillance du comportement et du principe de la bonne foi.

De notre point de vue, l'enregistrement, l'observation, l'analyse, la sauvegarde et le traitement ultérieur d'informations et d'activités de toutes sortes sur l'ordinateur sans le consentement de la personne concernée constituent une violation du domaine secret ou du domaine privé par des appareils d'enregistrement au sens du code pénal. Le fait de doter l'ordinateur de fonctions de surveillance et d'enregistrement en fait un appareil d'enregistrement. La sphère privée sur le lieu de travail est protégée tant en vertu du droit du travail, qu'en vertu du secret des télécommunications garanti par la constitution (voit ATF 126 I 50). Etant donné la multitude des fonctions et possibilités de programmation des systèmes de surveillance, l'atteinte à la personnalité de l'employé peut être, selon les circonstances, plus grave que par la mise en place d'une caméra-vidéo. Le Tribunal fédéral n'a encore pas rendu d'arrêt sur les programmes électroniques de surveillance.

7.3 La gestion des courriels durant les absences et en cas de départ de l'entreprise

Un bon déroulement de la marche des affaires d'une entreprise nécessite que les entrées et les sorties des documents soient systématiquement enregistrées et suivies. Au poste de travail, il n'est pas toujours possible de faire la différence entre courriels privés et professionnels, raison pour laquelle la gestion du courrier électronique des employés durant leur absence est une source de difficultés sous l'angle de la protection des données. L'utilisation d'une adresse constituée à partir de la fonction de la personne en question et non de son nom peut permettre d'éviter ces problèmes.

Dans le domaine du courrier électronique, tout comme dans la correspondance postale usuelle, il existe deux modes d'adressage: d'après le nom (par ex. jean.dupont@firme.ch ou jean.dupont@vente.firme.ch) ou d'après la fonction, donc sans nom (par ex. info@firme.ch, vente@firme.ch ou encore chefdevente@firme.ch) L'adresse constituée à partir du nom est aujourd'hui la plus répandue.

En cas d'adresse nominale, la gestion des courriels en l'absence de l'employé concerné ou en cas de départ de l'entreprise est une source de problèmes car il est difficile de faire la différence entre les courriers électroniques privés et professionnels. Si aucune mention ne permet de les différencier et si la nature privée du courrier sur la base des éléments d'adressage n'est ni reconnaissable, ni sûre, l'employeur peut – tout comme en cas de courrier postal classique – partir du principe que le courrier est professionnel. S'il existe des doutes fondés sur la nature d'un courriel, l'employeur doit tirer le cas au clair avec l'employé. Dans un tel cas, il lui est interdit de prendre connaissance du courrier électronique, que la correspondance électronique privée soit autorisée ou non.

Quant aux absences prévues (par ex. vacances, congés, service militaire), il existe essentiellement trois genres de gestion des courriels:

- Une réponse est définie dans le programme de courrier électronique: elle est envoyée automatiquement à l'expéditeur de chaque message entrant, précise la durée de l'absence et donne les coordonnées de la personne à contacter en cas d'urgence.
- Le programme de courrier électronique est constitué de telle sorte que tous les messages entrants sont dirigés vers un suppléant défini à l'avance. Cette solution comporte le risque que des courriels privés parviennent également chez le suppléant désigné.

- Un suppléant est désigné: il possède une autorisation restreinte lui permettant de consulter uniquement les courriels professionnels entrants; il peut éventuellement en poursuivre le traitement. Les courriels indiqués comme étant privés ne sont pas accessibles au suppléant. La sphère privée du collaborateur absent demeure ainsi préservée.

En cas d'absence imprévue (par ex. maladie, accident), un suppléant devrait être choisi à l'avance.

L'adresse non nominative est appropriée à la correspondance professionnelle non personnelle car elle contourne les difficultés liées à l'adresse nominative. L'adresse nominative ne devrait être utilisée que pour l'échange purement personnel d'informations professionnelles (par ex. pour les affaires concernant le personnel ou les communications personnelles).

Avant de quitter une entreprise, un collaborateur doit transmettre au niveau interne par courrier électronique toutes les affaires en suspens. L'employé doit confirmer la transmission de tous ces documents à l'entreprise. Il a la possibilité de sauvegarder ses courriels privés et autres documents privés sur des supports de données privés et de les effacer du serveur de l'entreprise.

En cas de départ, au plus tard le dernier jour de travail, il faut que son adresse électronique soit bloquée (comme tous ses autres comptes électroniques) et sa boîte aux lettres électronique effacée (comme tous ses autres supports de données personnels). L'employeur devrait s'y engager par écrit. Les personnes qui envoient des courriers électroniques à l'adresse bloquée sont dans ce cas automatiquement informées que l'adresse du destinataire n'est plus valable.

7.4 Protection de la sphère privée lors de l'utilisation du disque virtuel personnel

Les employés utilisent souvent à des fins privées leur disque virtuel personnel (home drive) dans le réseau de leur entreprise. De ce fait, ils occupent naturellement une capacité de sauvegarde qui – surtout lorsque la quantité de données enregistrée est grande – incite bon nombre d'employeurs à vérifier l'utilisation privée du disque virtuel personnel.

Le disque virtuel personnel ne doit en principe être utilisé que pour des documents professionnels ou à la fois personnels et professionnels. Les documents privés par contre doivent être transférés sur des supports de données privés. L'employé a ainsi la possibilité de se protéger contre l'accès illicite de tiers. L'accès à des documents personnels et professionnels dans le disque virtuel personnel par des supérieurs hié-

rarchiques ou des informaticiens n'est admis qu'en cas de nécessité et à la condition qu'il existe un motif justificatif et un règlement d'accès.

De même que pour l'utilisation du courrier électronique au poste de travail, il est ici recommandé d'établir une limitation de la capacité de sauvegarde (quota disque) personnelle, adaptée aux besoins des collaborateurs. Les quotas disque bloquent l'extension excessive de la capacité de sauvegarde revendiquée et empêchent une durée démesurément longue de conservation de documents. Les quotas disque obligent l'utilisateur à gérer sa capacité de sauvegarde personnelle et à effacer régulièrement ou à transférer sur d'autres supports de données (par ex. disquettes) les documents inutiles.

7.5 Protection des données et utilisation de l'agenda électronique au poste de travail

L'agenda électronique au poste de travail peut être une source de problèmes. Des données privées sont mêlées aux informations professionnelles et synchronisées à l'ordinateur au poste de travail. En particulier les règles d'accès à ces données constituent une difficulté.

Du fait des règles d'accès internes, les agendas électroniques sont en général consultables par un grand nombre de personnes, dans la plupart des cas secrétaires ou supérieurs hiérarchiques, mais aussi bien souvent par tous les collaborateurs. Un agenda peut néanmoins contenir des informations qui ne doivent pas être librement accessibles à des tiers. Ce n'est pas seulement la sphère privée de l'employé qui est touchée, mais aussi des données qui lui appartiennent, à la fois professionnelles et personnelles, ou des informations privées sur des tiers (par ex. les anniversaires). La sphère privée n'est en général accessible qu'à un cercle restreint de connaissances ou à un nombre limité d'ayants droit. La personne concernée a le droit de déterminer elle-même avec qui elle désire partager sa sphère privée (droit à l'autodétermination individuelle en matière d'information). Pour éviter qu'il ne soit consulté par des collègues de travail ou des supérieurs hiérarchiques, le domaine privé doit être expressément caractérisé comme tel. La mention «Privé» protège le contenu des données privées de la consultation de tiers. Mais le fait qu'un collaborateur ait introduit des données privées demeure néanmoins visible.

En cas d'absence du consentement de la personne concernée, les données privées des agendas électroniques concernant des tiers ne peuvent être consultées qu'en présence d'un intérêt prépondérant privé ou public.

7.6 Analyses génétiques sur le lieu de travail

Les analyses médicales, dont relèvent aussi les analyses génétiques (les analyses présymptomatiques), peuvent s'avérer importantes lors de l'élaboration de prescriptions visant la protection de la santé et la sécurité dans des secteurs d'activité à risque considérable pour la santé ou la sécurité. Le traitement de données génétiques sur le lieu de travail est réglementé dans le projet de loi fédérale sur l'analyse génétique humaine. La collecte de données génétiques peut constituer une violation de la personnalité contraire au droit.

Les analyses génétiques ont pour but de déterminer une prédisposition génétique pouvant s'avérer importante dans les activités professionnelles d'employés ou de candidats.

Les contrôles génétiques sont fondés sur des analyses génétiques régulières. L'objectif d'un contrôle génétique est d'anticiper le risque de déclenchement d'une maladie ou de détecter des stades précoces de lésions génétiques (par ex. les mutations génétiques). Certains employés qui sont exposés régulièrement à certaines substances ou dangers sur le lieu de travail peuvent faire l'objet d'une surveillance génétique.

Dans les pays où les analyses génétiques se pratiquent déjà, les informations génétiques sont utilisées à diverses fins. Par exemple pour refuser des candidats «au patrimoine génétique défavorable» ou pour déplacer des employés à des postes de travail impliquant moins de risques. C'est le cas de l'analyse génétique portant sur la réceptivité à l'asthme de candidats appelés à travailler dans un environnement où la poussière est présente (par ex. dans une boulangerie). Souvent, il s'agit aussi d'éviter des pertes de productivité dues à l'absentéisme. Les données génétiques sont aussi utilisées à des fins d'identification. En Angleterre par exemple, les données génétiques d'employés ou de stagiaires de police sont comparées aux traces génétiques trouvées sur le lieu de l'infraction dans le but d'éviter d'éventuelles contaminations ultérieures des moyens de preuves. Aux Etats-Unis, des échantillons génétiques sont utilisés pour identifier les soldats morts au combat. Les membres de l'armée peuvent demander la destruction de leurs relevés génétiques dès qu'ils quittent l'armée. L'employeur utilise également les informations génétiques dans le but de protéger la santé et la sécurité de tiers.

Diverses voix se sont déjà élevées contre les analyses génétiques. Tout d'abord, l'utilisation d'informations génétiques peut avoir pour conséquence l'exclusion de branches professionnelles spécifiques à des employés chez qui l'on décèle certaines prédispositions génétiques. Mais être prédisposé génétiquement à une maladie ne signi-

fie pas obligatoirement que les symptômes en question surgiront véritablement. Il est aussi possible que d'autres employeurs ou assureurs aient un comportement discriminatoire lorsque les données génétiques leurs sont communiquées (perte de contrôle sur ses propres données génétiques). Au lieu de contribuer à décharger le domaine de la santé et des assurances sociales, cela contribuerait plutôt à lui imposer un fardeau supplémentaire (notamment à l'assurance-chômage). Il y a néanmoins un intérêt public à protéger la personne quant à son droit au travail tout comme à protéger le secteur de la santé et des assurances sociales.

Le traitement de données génétiques peut aussi constituer un risque pour la personnalité. D'une part, les tests génétiques constituent une mesure incisive pouvant léser l'intégrité physique. D'autre part, la collecte d'informations génétiques peut constituer une atteinte à la sphère privée en matière d'informations, pour la personne concernée et sa famille. Dans ce contexte, la protection de la sphère privée doit être considérée en tant qu'intérêt public. Alors que la sphère privée est en général comprise en tant que droit individuel, l'atteinte à la sphère privée d'un grand nombre de personnes a un impact sur la société toute entière. Par ailleurs, il convient de considérer qu'en raison du rapport de dépendance de l'employé envers son employeur, on ne peut pas simplement considérer qu'un éventuel consentement a été donné véritablement librement par la personne concernée. Une analyse génétique pourrait aussi violer le droit d'ignorer sa propre prédisposition génétique. Il se peut aussi qu'il n'y ait pas de lien entre le travail effectué et le déclenchement d'une maladie déterminée. Il n'est donc pas sûr qu'une analyse génétique pourra livrer de meilleures indications que les contrôles de santé usuels. Dans la plupart des cas, il est plus judicieux d'éliminer les sources de risques et de dangers que de procéder à d'inutiles analyses génétiques.

L'employeur devrait éviter d'introduire un programme de test génétique onéreux sans que la valeur des informations ainsi obtenues ait été clairement déterminée. Par ailleurs, les analyses génétiques risquent de supplanter les prescriptions usuelles en matière de santé et de sécurité du droit du travail. Jusqu'à ce jour, nous n'avons encore jamais été informés d'un cas concret d'analyses génétiques sur le lieu de travail en Suisse. Néanmoins, le traitement de données génétiques sur le lieu de travail est d'ores et déjà réglé dans le projet de loi fédérale sur l'analyse génétique humaine. Cette loi interdit expressément toute discrimination d'une personne en raison de son patrimoine génétique. En outre, le projet pose des conditions sévères aux tests génétiques effectués sur le lieu de travail: ceux-ci ne peuvent avoir lieu qu'avec le consentement écrit de la personne concernée et ils sont proscrits si d'autres méthodes (par ex. le relevé de données sur les antécédents médicaux des membres de la famille) permettent d'obtenir les informations requises (principe de la proportionnalité).

Le projet de loi fédérale prévoit également que les analyses présymptomatiques ne peuvent être effectuées que dans les cas où une maladie professionnelle, des risques d'une atteinte grave à l'environnement ou des risques majeurs d'accident ou d'atteinte à la santé de tiers sont susceptibles de se produire en relation avec la place de travail. En outre, les analyses génétiques ne sont admissibles que si d'autres mesures de la loi sur l'assurance-accidents ou d'autres dispositions légales ne suffisent pas pour exclure les risques de maladie ou d'accident. La place de travail devra par ailleurs être soumise aux prescriptions sur la prévention dans le domaine de la médecine du travail en vertu d'une décision de la SUVA ou de dispositions légales. Le projet de loi établit enfin que le mode d'analyse doit être qualifié de sûr et de fiable par une commission fédérale d'experts pour l'analyse génétique humaine. Le législateur a soumis le traitement de données génétiques au secret professionnel et lié sa violation à des sanctions pénales.

8. Economie et commerce

8.1 Publicité non désirée par courrier électronique (spam)

Les messages électroniques publicitaires représentent aujourd'hui une part importante du volume du courrier électronique. Quiconque ne désire pas recevoir ces messages, réalise souvent qu'il n'est pas facile à obtenir que certains annonceurs cessent leurs envois.

La publicité par courrier électronique non sollicitée et donc en partie non désirée constitue un phénomène de masse notamment parce que l'expéditeur est capable, avec un minimum d'effort et de moyens financiers, d'atteindre un nombre extrêmement élevé de destinataires. L'aspect problématique de ce système est que ceci engendre des efforts et des coûts (frais de connexion, examen et suppression des messages reçus, espace occupé sur le disque) auprès des destinataires, dont une partie au moins ne désire pas recevoir cette publicité.

Selon la situation juridique actuelle en Suisse, deux conditions doivent au moins être remplies pour qu'un envoi non sollicité de courriel publicitaire puisse être considéré comme licite. Premièrement, seules des adresses collectées de manière licite peuvent être utilisées. Cela signifie en particulier qu'à part les adresses, dont le propriétaire a consenti à ce qu'elles soient utilisées à des fins publicitaires par certains annonceurs ou pour certains domaines d'intérêt, les seules adresses utilisables sont celles tirées d'annuaires publics dont les conditions d'utilisation n'excluent pas une utilisation à des fins publicitaires. Doivent par contre être considérées comme ayant été collectées de manière illicite les adresses dont le propriétaire a explicitement ou

implicitement manifesté qu'il ne désirait pas qu'elles soient utilisées à des fins publicitaires. Un exemple d'une manifestation explicite est par ex. une mention du genre «pas de publicité» ou «no address grabbing» apposée sur un site web. Une opposition implicite peut sans doute être admise dans tous les cas ou l'usage prévu d'une adresse est spécifique et non lié à la publicité. Deuxièmement, les destinataires des messages publicitaires doivent en tout temps avoir un moyen simple de faire valoir leur droit à l'effacement des données. Bien sûr, la solution la plus simple et la plus appropriée au moyen de communication utilisé est d'indiquer dans le message même une adresse de courriel par l'intermédiaire de laquelle ceci peut être effectué. Cette exigence est également stipulée dans les règles – en particulier la règle n° 4.4 – de la Commission suisse pour la loyauté (http://www.lauterkeit.ch/pdfF/grundsaetzeF.pdf). C'est précisément cette exigence de disposer d'un moyen simple pour faire effacer les données que de nombreux expéditeurs de messages publicitaires ne remplissent pas. Dans notre recommandation du 24 janvier 2003, nous avons formellement invité l'annonceur résidant à Zurich, mentionné dans notre 9ème rapport d'activités, à conformer son activité commerciale et ses traitements de données aux dispositions légales. Cette recommandation est publiée dans l'annexe de ce rapport (paragraphe 13.7.3).

En Suisse, les voies de droit offertes aux personnes qui désirent s'opposer à la publicité indésirable sont (encore) limitées (cf. notre feuillet thématique sur le spam sur www.edsb.ch). Pour intenter une action contre les annonceurs du secteur privé, il faut suivre la voie du droit civil, ardue parce qu'elle cause souvent des frais importants sans pour autant donner une garantie quant à l'issue. Il y a 3 ans, le Conseil fédéral a accepté une motion (cf. motion 00.3393) à ce sujet qui demandait que l'on modifie la situation juridique. Il est prévu, dans le cadre de la révision de la loi sur les télécommunications (LTC), d'introduire un article correspondant dans la loi fédérale contre la concurrence déloyale (LCD). La situation dans les pays limitrophes est quelque peu différente. La France par exemple connaît un régime nettement plus sévère. Ainsi, les fichiers d'adresses doivent être communiqués à l'autorité de surveillance – la CNIL (Commission Nationale de l'Informatique et des Libertés) - et une violation des dispositions réglant la collecte ou la communication licites d'adresses peut entraîner des conséquences pénales (jusqu'à 5 ans de prison et 300'000 euros d'amende). Vous trouverez plus d'informations sur le site web de la CNIL (http://www.cnil.fr). Quant à la CE, elle a ancré dans sa directive 2002/58/CE le principe du consentement préalable et les Etats membres doivent avoir transposé cette directive dans leur droit national d'ici au 31 octobre 2003. Dans certains pays (Autriche, Danemark, Finlande et Italie), ce principe est déjà appliqué en vertu de réglementations existantes.

9. Finances

9.1 Service d'information sur le crédit à la consommation

La loi sur le crédit à la consommation prévoit la création d'un service d'information sur le crédit à la consommation dont la tâche consistera à gérer un fichier électronique contenant des indications sur des personnes qui ont bénéficié d'un crédit à la consommation. Ce service ne peut se contenter de régler le traitement des données dans ses statuts, mais comme tout autre organe fédéral, il doit disposer de bases légales suffisantes. Une information transparente sur le volume des données traitées et les personnes chargées du traitement en fera partie.

La nouvelle loi fédérale sur le crédit à la consommation est entrée en vigueur le 1er janvier 2003. Elle ne porte pas seulement sur les crédits en liquide et les contrats de paiement partiels (par ex. les contrats de leasing), mais également sur les cartes de clients et cartes de crédit ainsi que les crédits consentis sous la forme d'une avance sur compte courant, liés à la possibilité de rembourser le solde par paiements partiels. La loi ne s'applique que lorsque le prêteur consent, par métier, un crédit à la consommation et que le consommateur utilise ce crédit à des fins privées et non dans un but professionnel ou commercial.

D'une part, les prêteurs sont légalement tenus de contrôler la capacité de contracter un crédit des futurs consommateurs, et ceci avant la conclusion du contrat; par ailleurs, ils doivent annoncer tous les crédits consentis à un service central. Pour ces raisons, les prêteurs se sont regroupés et ont formé une institution commune qui a pour nom «centre de renseignements sur le crédit à la consommation» (centre de renseignements). Le centre de renseignements gère toutes les données recueillies dans un fichier électronique, le système d'information sur les crédits à la consommation. Ce système d'information contient tous les renseignements personnels sur les consommateurs (nom, prénom, date de naissance, adresse) ainsi que des données sur le crédit à la consommation contracté (type de crédit, début et fin du contrat, nombre de versements, montant brut du crédit, montant des versements, etc.). Les prêteurs peuvent également accéder aux données personnelles traitées par une procédure d'appel (par ex. dans le cadre d'un examen de la capacité de contracter un crédit).

Le centre de renseignements est certes un organe privé, mais selon la loi sur le crédit à la consommation, c'est également un organe fédéral au sens de la loi sur la protection des données. De ce fait, nous avons dû rappeler à diverses reprises que le centre nécessitait une base légale suffisante pour le traitement de données. Les statuts d'un

organisme privé ne suffisent pas. Nous nous sommes engagés pour que le centre de renseignements soit tenu de respecter les mêmes règles pour le traitement de données que les autres organes fédéraux. Nous avons en définitive réussi à imposer que les détails du traitement des données soient établis clairement dans l'ordonnance relative à la loi sur le crédit à la consommation et que l'annexe de l'ordonnance contienne la liste complète des données, l'étendue de l'accès et l'autorisation de traiter les données. En outre, le centre de renseignements doit tenir une liste des prêteurs admis à utiliser la procédure d'appel, tenir cette liste constamment à jour et la rendre accessible à tous. A notre suggestion, le centre s'est déclaré en outre prêt à publier les statuts ainsi que le règlement concernant le déroulement des échanges avec le centre de renseignements.

Le centre est responsable du système d'information sur le crédit à la consommation. Conformément à la loi sur la protection des données, il est donc tenu de veiller à ce que de fausses données ne soient pas communiquées et que les noms des consommateurs soient immédiatement effacés dès que le crédit à la consommation est payé.

Le Département fédéral de justice et police a approuvé les statuts du centre de renseignements et le règlement mentionné. Nous avons apporté une réserve à ce propos étant donné qu'un examen définitif des traitements de données effectué par le centre ne pourra avoir lieu que lorsque le règlement de traitement requis par la loi sur la protection des données sera établi.

9.2 Clauses de consentement dans les demandes de cartes de crédit

Les clauses de consentement que l'on trouve dans les conditions générales sont un sujet de discussion permanent au sein de la protection des données, car elles traitent souvent de la collecte et de la communication de données. A part les clauses contenues dans les demandes d'assurance et dans le domaine des télécommunications, ce sont surtout les clauses contenues dans les demandes de carte de crédit qui récemment soulèvent des inquiétudes.

Nous avons reçu plusieurs plaintes de personnes concernées relatives aux clauses de consentement des conditions générales de demandes de carte de crédit. Il s'est avéré que diverses versions de ces conditions générales contiennent effectivement des éléments inquiétants. Nombre de ces clauses contiennent des formulations absolument opaques qui laissent douter de la validité juridique d'un consentement donné en vertu d'une telle clause. Finalement, un consentement ne peut être valable que dans la mesure où la personne concernée est capable d'en mesurer la portée concrète. Une clause qui prévoit qu'un client donne son accord pour que ses données soient traitées par des tiers, qui ne sont pas explicitement désignés, dans le but de dévelop-

per des prestations de service qui seraient enclins à réveiller son intérêt, ne peut certainement pas être considéré comme satisfaisant du point de vue de la protection des données. Il faut déplorer le fait que ces dernières années les diverses clauses soient devenues de plus en plus floues et que le degré de clarté varie fortement d'un émetteur de cartes de crédit à un autre. Nous sommes d'avis que les mêmes règles devraient être appliquées pour les divers émetteurs de cartes, qui sont d'ailleurs en situation de concurrence.

10. Statistique et recherche

10.1 Communication de données statistiques à d'autres unités administratives

L'utilisation de données statistiques à des fins de surveillance est autorisée si elle est explicitement prévue par une disposition d'une loi fédérale ou si elle reçoit le consentement écrit des personnes concernées. Si les données utilisées à des fins statistiques sont collectées en même temps que les données utilisées à des fins de surveillance, le principe de transparence exige qu'il soit clair quelles données sont également ou exclusivement utilisées à des fins de surveillance et transmises à d'autres offices. Nous sommes d'avis que les bases légales réglant la transmission de données en provenance de la statistique des fournisseurs de prestations de l'OFS à d'autres offices, en particulier à l'OFAS, ne sont pas suffisamment précises. Un avis de droit du service juridique du DFI parvient à une conclusion opposée et autorise la communication.

L'OFS élabore de nombreuses statistiques dans le domaine de la santé, entre autres la statistique des fournisseurs de prestations (statistique des hôpitaux). Depuis l'introduction de la loi sur l'assurance-maladie (LAMal), ces données sont également utilisées à des fins de surveillance dans le cadre de l'application de la LAMal. Selon la loi sur la statistique fédérale, l'utilisation de données statistiques à des fins de surveillance n'est cependant autorisée que si elle est explicitement prévue par une disposition d'une loi fédérale ou si les personnes concernées ont donné leur consentement écrit pour un traitement à d'autres fins. (cf. 4ème rapport d'activités 1996/97, chapitre I.6.2; 5ème rapport d'activités 1997/98, chapitre II.8.6; 6ème rapport d'activités 1998/99, chapitre I.8.3).

Les dispositions prévues dans la LAMal ainsi que dans l'ordonnance sur l'assurance-maladie ne se réfèrent à notre avis qu'à une collecte directe des données par l'OFAS. Elles ne sont pas assez précises en ce qui concerne la communication des données

de l'OFS à l'OFAS; elles ne stipulent notamment pas si les données transmises par l'OFS doivent permettre une identification de l'hôpital concerné ou non. Etant donné que les collectes de données effectuées par l'OFS englobent aussi bien les données utilisées à des fins statistiques que celles utilisées à des fins de surveillance, le principe de transparence exige qu'il soit clair pour les fournisseurs de données (hôpitaux) quelles données sont aussi ou exclusivement utilisées à des fins de surveillance et ensuite transmises sous forme non anonymisée à l'OFAS ou à d'autres offices.

Il est donc nécessaire du point de vue de la protection des données soit d'adapter les bases légales, soit de demander le consentement écrit des hôpitaux concernés pour la communication des données.

Après de longues et difficiles discussions que nous avons menées avec les divers offices, le service juridique du secrétariat général du DFI a émis un avis de droit dans lequel il retient que les bases légales existantes pour la communication des données sont suffisantes, ce autant pour la communication à l'OFAS que pour celle à d'autres offices chargés d'exécuter, de contrôler ou de surveiller l'exécution de la LAMal (tel que le surveillant des prix). Nous maintenons cependant notre position.

11. International

11.1 Conseil de l'Europe

11.1.1 Travaux du CJPD: vidéosurveillance, carte à puce, données policières et données judiciaires en matière pénale

Le Groupe de projet sur la protection des données (CJPD) s'est réuni du 7 au 9 octobre 2002. Il a adopté un projet de lignes directrices régissant la protection des données dans le cadre de la vidéosurveillance.

Lors de sa 40ème réunion, le CJPD a adopté un projet de lignes directrices régissant la protection des données dans le cadre de la vidéosurveillance. Ces lignes directrices énoncent les principes à prendre en considération lors du recours à des activités de vidéosurveillance par des autorités publiques ou des personnes privées. Elles définissent également des garanties à l'égard des personnes concernées. Le CJPD a également adopté un rapport sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale, ainsi qu'un rapport sur la troisième évaluation de la recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Ces deux rapports précisent le contenu des principes de base de la protection des données dans ces secteurs. Le

CJPD a poursuivi ses travaux en vue de l'adoption de lignes directrices régissant l'utilisation de cartes à puce. Il s'est finalement penché sur ses structures et méthodes de travail.

11.1.2 Travaux du T-PD: clauses contractuelles – évaluation de la Convention 108

Le Comité consultatif de la Convention 108 (T-PD) a tenu sa 18ème réunion du 9 au 11 octobre 2002. Il a adopté un guide régissant les clauses contractuelles en matière de flux transfrontières des données et poursuivi ses travaux d'évaluation de la Convention.

Sous présidence suisse, le T-PD a adopté un guide régissant les clauses contractuelles en matière de flux transfrontières des données. Ce guide est un instrument important dans le contexte des transferts de données vers des Etats n'assurant pas un niveau de protection des données adéquat. Ce guide complète le contrat-type adopté par le T-PD en 1992. Il donne des lignes directrices lors de l'élaboration de clauses contractuelles. Il ne s'agit pas d'un instrument juridique contraignant. Il doit ainsi permettre aux exportateurs résidant dans un pays ayant ratifié la Convention 108 de rédiger des clauses contractuelles de protection des données qui soient conformes aux exigences de la Convention 108 et de son protocole additionnel. Ces clauses contractuelles doivent en particulier contenir des garanties pour le respect des droits des personnes dont les données sont transférées vers des Etats tiers n'offrant pas un niveau de protection des données satisfaisant. Le T-PD complètera l'instrument en fonction des évolutions à venir.

Le T-PD a en outre entériné les résultats de la Conférence d'évaluation de la Convention 108 qui s'est tenue à Varsovie en novembre 2001 (voir 9ème rapport d'activités, paragraphe 11.1.2). En particulier, il estime que les principes de la Convention 108 sont toujours pertinents et qu'il ne convient pas de remettre en question les réalisations de la Convention. Il propose néanmoins de poursuivre l'analyse des principes de la Convention et de voir dans quelle mesure ils répondent aux questions soulevées par les développements technologiques. Il mettra ainsi l'accent sur les droits des personnes concernées, l'analyse des flux transfrontières de données, les conséquences des nouvelles technologies et l'examen des dérogations légitimes à certains principes de base de la protection des données prises sur la base de l'article 9 de la Convention. Le T-PD s'est enfin penché sur les structures de la protection des données au Conseil de l'Europe et sur ses méthodes de travail.

11.1.3 Conférence sur les défis et les problèmes posés aux nouvelles autorités de contrôle de protection des données

Du 12 au 13 décembre 2002 s'est tenue à Madrid une conférence sur les défis et les problèmes posés aux nouvelles autorités de contrôle de protection des données, organisée par le Conseil de l'Europe et l'Agence de protection des données de l'Espagne. Nous y avons participé et présenté un rapport sur les défis posés par les flux transfrontières de données à caractère personnel.

Répondant à une demande des Etats membres du Conseil de l'Europe qui ont adopté récemment une législation de protection des données et mis en place une autorité de protection des données, le Conseil de l'Europe et l'Agence de protection des données de l'Espagne ont organisé une conférence sur les défis et les problèmes posés aux nouvelles autorités de contrôle de protection des données. Cette conférence réunissait des représentants de nouvelles autorités de contrôle de 15 pays d'Europe centrale et orientale, de Chypre et de Malte, ainsi que des représentants d'autorités de protection des données de la France, de l'Espagne, de l'Italie, du Portugal, des Pays-Bas, du Québec et de la Suisse (PFPD et Préposé du canton de Zoug). L'OCDE et la Commission européenne ont également pris part aux travaux. Cette conférence a permis un échange utile et fructueux d'informations entre autorités ayant une longue expérience dans l'application des règles de protection des données et les nouvelles autorités. Elle a permis en particulier d'aborder les questions de mécanisme de mise en œuvre des principes de la protection des données, des compétences et du rôle des autorités de contrôle, de leur organisation, de leur degré d'indépendance et des conditions de leur indépendance. Il a ainsi été rappelé que l'indépendance est une condition fondamentale pour permettre aux autorités de protection des données d'accomplir leurs tâches, car ces autorités ont été mises en place pour défendre les droits de l'homme dans le contexte des traitements de données personnelles. L'indépendance couvre non seulement la fonction, mais également la nature de l'autorité. L'indépendance ne signifie pas uniquement l'autonomie dans l'action. Le niveau de l'indépendance se mesure également par rapport aux moyens octroyés à l'autorité, notamment budgétaire et de la marge de manœuvre à disposition dans la gestion de ces moyens. La Conférence a également débattu des problèmes que les autorités peuvent rencontrer dans leurs relations avec les responsables de traitement, ainsi que le rôle des autorités de contrôle dans les structures fédérales avec notamment une contribution du préposé à la protection des données du canton de Zoug. Enfin, elle s'est penchée également sur les défis posés par les flux transfrontières de données. Nous avons dans ce cadre présenté un rapport décrivant la réglementation de la Convention 108 et du protocole additionnel régissant les flux transfrontières ainsi

que les réglementations nationales à la lumière de la législation de quelques Etats parties à la Convention. Nous nous sommes également interrogés sur le rôle des autorités de protection des données dans le contexte des flux transfrontières (le rapport est publié sur notre site www.edsb.ch et sur le site du Conseil de l'Europe www.coe.int/dataprotection). Nous avons en particulier souligné qu'à l'avenir, les autorités de contrôle devraient avoir un rôle plus proactif et s'attacher à sensibiliser les personnes concernées et les responsables de traitement aux risques liés aux flux transfrontières de données. La Conférence a permis dans ce contexte de rappeler l'importance de la collaboration internationale entre autorités nationales de protection des données pour répondre aux défis d'une société globalisée.

11.1.4 Projet de protocole sur la génétique humaine

Un groupe de travail du Conseil de l'Europe travaille actuellement à l'élaboration du protocole sur la génétique humaine. Une partie du protocole est désormais achevée et doit être soumise pour avis aux milieux intéressés.

Plusieurs protocoles additionnels à la Convention du Conseil de l'Europe sur les droits de l'homme et de la biomédecine (Convention d'Oviedo) sont prévus. L'un d'entre eux, le protocole sur la génétique humaine, a pour but de réglementer les analyses génétiques dans le domaine médical ainsi que dans le domaine du travail et des assurances (voir également le 9ème Rapport d'activités 2001/2002, paragraphe 11.1.4).

Au cours de l'année écoulée, le groupe de travail a examiné l'éventualité de publier dès maintenant certaines parties du protocole. Il a décidé en définitive de remanier une fois encore le chapitre I (Dispositions générales) et le chapitre II (Domaine médical) et de les transmettre pour avis aux milieux intéressés. Le rapport explicatif qui accompagne ces deux chapitres sera également soumis à la discussion. Le groupe de travail répond ainsi aux vœux du Comité des Ministres du Conseil de l'Europe.

Citons parmi les thèmes traités dans les chapitres mentionnés le consentement des personnes concernées, les normes de qualité auxquelles doivent répondre les analyses génétiques, la consultation génétique, la conservation de matériel biologique (y compris les données génétiques) et la transmission éventuelle de données génétiques aux membres de la famille. En outre, des règles ont été établies à propos des dépistages génétiques et de la thérapie génétique. Il sera également établi à quelles conditions les analyses génétiques peuvent être effectuées auprès des personnes incapables de discernement. Les prochaines réunions seront l'occasion pour le groupe de travail de se pencher sur les analyses génétiques dans le domaine du travail et des assurances, qui font également partie du protocole.

11.2 Union européenne

11.2.1 Négociations bilatérales II entre la Suisse et l'Union européenne

Nous suivons de près les négociations sur les services et celles relatives à l'adhésion aux Accords de Schengen et de Dublin, qui nécessiteront, en cas d'accord, une reprise de l'acquis européen sur la protection des données. Les services de la Commission européenne ont entamé un examen comparatif du droit européen et de la législation suisse. Voir aussi paragraphe 1.1.

11.2.2 Conférence européenne des commissaires à la protection des données

Les commissaires européens à la protection des données se sont réunis à Bonn, les 25 et 26 avril 2002 et à Cardiff, le 9 septembre 2002. Nous y avons participé en tant qu'observateur. La Conférence a adopté une déclaration relative à la conservation systématique et obligatoire des données de trafic des télécommunications.

La Conférence européenne des commissaires à la protection des données réunit les commissaires des pays membres de l'Union européenne, de la Norvège et de l'Islande. La Hongrie, la Pologne, la République tchèque et la Suisse y ont le rang d'observateur. Elle permet un échange approfondi sur l'évolution des législations de protection des données en Europe, sur les développements technologiques, notamment les technologies favorables à la protection des données et les pratiques des autorités de protection des données. Elle débouche également sur l'élaboration de solutions communes et l'adoption de déclarations sur des thèmes d'actualité.

La Conférence de Bonn a permis de faire le point sur les mesures prises suite aux attentats du 11 septembre 2001. Les commissaires ont noté avec satisfaction que dans l'ensemble aucune mesure disproportionnée et inconsidérée n'avait été prise, mais ont convenu de la nécessité de rester vigilant, car plusieurs projets législatifs étaient en préparation dans les différents Etats. Ils ont notamment constaté que les Etats avaient une approche similaire dans l'utilisation de la biométrie à des fins de police et qu'en particulier les mesures législatives adoptées étaient limitées dans le temps et feraient l'objet d'évaluation. Les commissaires ont pris connaissance des développements techniques dans le domaine de l'identification biométrique et constaté que la technologie permettait des percées encourageantes pour protéger la vie privée des individus. Il est ainsi possible de recourir à des installations de vidéosur-

veillance qui permettent de garantir l'anonymat des personnes filmées aussi longtemps qu'une identification n'est pas nécessaire.

La Conférence a également pris connaissance des projets concernant la certification et les labels de qualité «protection des données», notamment en Allemagne et au Pays Bas. Ils ont estimé nécessaire de développer des stratégies communes qui pourraient déboucher sur un concept européen de certification. Enfin, les commissaires ont eu un échange de vue sur différents thèmes d'actualité dans les différents Etats membres et notamment le gouvernement électronique et l'utilisation du numéro d'identification personnelle (NIP).

En marge de la Conférence internationale des commissaires à la protection des données à Cardiff (voir paragraphe 11.4.1), les commissaires européens ont adopté une déclaration relative à la conservation systématique et obligatoire des données de trafic des télécommunications (voir paragraphe 13.6). En particulier, ils rappellent que lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée. La période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou toute autre forme d'abus. La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable.

11.2.3 Groupe de travail européen sur le traitement des plaintes et les échanges d'informations

Nous avons poursuivi notre participation aux travaux menés par le groupe de travail créé dans le cadre de la Conférence européenne des Commissaires à la protection des données et destiné à examiner les moyens de collaboration entre autorités de contrôle de protection des données lors de l'examen des plaintes qu'elles traitent et des inspections qu'elles effectuent. Ces travaux ont en particulier porté sur la comparaison des compétences de contrôles nationales respectives ainsi que sur les réglementations des flux transfrontières.

Nous avons continué notre activité au sein du groupe de travail européen «traitement des plaintes et échanges d'informations» (Complaints handling Workshop) en participant aux réunions qui se sont tenus au printemps et en automne 2002 à Dublin et Berlin. Sur la base du mandat attribué par la Conférence européenne des Commissaires à la protection des données, ce groupe de travail est chargé d'analyser les différentes méthodes de traitement des plaintes déposées auprès des autorités de protection des données et de favoriser la coopération entre ces dernières.

Lors de ces deux réunions, le groupe de travail a finalisé l'analyse comparative entamée à la réunion de Lisbonne en 2001 sur les procédures de contrôle mises en place par les différentes autorités de protection des données. Ces travaux ont permis d'élaborer un rapport de synthèse énumérant non seulement les méthodes utilisées par ces autorités pour effectuer leurs activités de surveillance mais également de comparer les différentes compétences légales de chacune d'entre elles. Ces travaux nous permettront d'une part de nous inspirer des solutions légales mises en place dans d'autres Etats et d'autre part de connaître les compétences d'investigation dont jouissent nos collègues étrangers en cas de demandes d'entraide lors de plaintes et d'enquêtes touchant à des traitements de données dépassant les frontières nationales. Nous avons également collaboré dans ce groupe de travail à l'élaboration de travaux comparatifs sur les nombreuses réglementations nationales touchant aux flux transfrontières de données.

Au cours de cette année, le système informatique CIRCA (Communication & Information Resource Centre Administrator) est devenu un instrument de collaboration extrêmement efficace pour les travaux du groupe de travail. Par l'intermédiaire de ce système extranet sécurisé lié au programme IDA (Interexchange of Data between Administrations) de la Commission européenne, nous avons pu procéder à de nombreux échanges d'informations concernant des solutions nationales trouvées à des problèmes similaires de protection des données, communiquer des résultats de contrôles effectués ou encore échanger des expériences utiles avec d'autres autorités de protection des données.

Lors de la réunion de Dublin, de nombreux intervenants ont en outre relevé l'importance de ne pas limiter ces échanges d'informations aux seuls membres de l'Union européenne mais d'ouvrir le système d'échange d'informations CIRCA ainsi que la participation au groupe de travail à d'autres Etats ayant un niveau de protection équivalent. Fort de cette ouverture, le groupe de travail s'est réuni à Berlin avec la participation des différents représentants des autorités de protection des données de l'Union européenne et de la Suisse ainsi que de nouveaux participants tels que la Tchéquie, la Slovaquie, la Slovénie, la Lituanie et la Pologne.

11.3 OCDE

11.3.1 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 abordé les thèmes suivants: la révision des directives sur la sécurité de l'information, l'authentification électronique, la sphère privée dans le commerce électronique, le lien entre mécanismes d'autorégulation et dispositions légales, la nécessité de réviser les directives en matière de cryptographie ainsi que le rôle de la biométrie dans la protection de la sphère privée.

Outre la publication, dans le cadre de la lutte contre le terrorisme, de nouvelles directives de sécurité, l'accent a été mis essentiellement sur la mise en œuvre d'une «culture de la sécurité» (culture of security) et, dans cette optique, sur l'élaboration de directives en matière de sécurité de l'information. Formulées de manière relativement générale, ces directives n'ont pas suscité de divergences fondamentales entre les Etats membres. Les principes qui caractériseront la sécurité de l'information des réseaux du futur ont donc été approuvés.

Après leur publication, les Etats membres et le Secrétariat ont pris les mesures nécessaires pour que ces directives touchent un public le plus large possible. En outre, plusieurs Etats membres se sont penchés sur la mise en application des principes de sécurité. Un point a fait l'unanimité: l'application concrète de ces principes au niveau du grand public doit s'accompagner de conseils pratiques concernant la sécurité des ordinateurs personnels. Dans cette optique, nous avons rajouté, sur notre site Internet à la rubrique «Thèmes», un chapitre consacré à la sécurité et publié, comme premier pas, des informations importantes relatives à la sécurité des ordinateurs personnels. De nombreux Etats membres ont pris des mesures similaires.

Par ailleurs, la délégation allemande a demandé une harmonisation de la politique de sécurité au niveau international et proposé de prendre en considération les travaux accomplis par l'UE dans le domaine de la sécurité. Dans ses conclusions, l'étude financée par l'UE sur les risques et les dépendances techniques souligne la nécessité d'établir des standards techniques minimaux, tout en précisant que ceux-ci doivent avoir une base légale. La position de l'OCDE sur les réglementations légales étant connue, cette étude a soulevé une certaine controverse.

En ce qui concerne l'authentification électronique, le groupe de travail a élaboré un document rassemblant les différents modèles et les dispositions légales. Cette liste a servi de base à l'élaboration des exigences légales fondamentales. En outre, la ques-

tion de l'interopérabilité des systèmes a été à nouveau abordée car peu de progrès ont été enregistrés dans ce domaine au cours des quatre dernières années. Le projet du gouvernement italien de rassembler une signature digitale, un numéro d'identification personnel (NIP) et une carte médicale a rencontré un grand intérêt.

La révision de la directive de l'OCDE sur la cryptographie sera suspendue pour quatre ans durant la poursuite des travaux sur l'authentification électronique.

Selon le rapport sur l'application de mesures visant la sécurité de la sphère privée dans le domaine du commerce électronique, présenté à la suite de la Conférence d'Ottawa (1999), la limite d'efficacité n'a été atteinte qu'en raison de l'impact restreint des dispositions légales sur la protection de la sphère privée. En revanche, les mécanismes d'autorégulation sont présentés dans le rapport – sans que ce résultat ne soit ni vérifié ni attesté – comme les seules mesures permettant de protéger efficacement la sphère privée. Nous avons demandé que le paragraphe concerné soit supprimé ou complété. En effet, bien que nous soyons convaincus que l'autorégulation sera appelée à jouer un rôle important dans le commerce électronique, nous estimons qu'outre les dispositions légales nationales, elle nécessite des normes reconnues au niveau international qui garantiront son efficacité.

Au cours des discussions que le groupe de travail a menées sur le programme des deux prochaines années, plusieurs pays membres ont suggéré de mandater des études de marché examinant les raisons de la méfiance à l'égard du commerce électronique. Ces discussions ont également souligné la nécessité d'analyser le caractère économique des mesures visant la protection de la sphère privée (à partir de quand la protection de la sphère privée s'avère-t-elle payante?). Nous avons souligné que la mise en œuvre de moyens visant la protection de la sphère privée ne doit pas être examinée uniquement sous l'angle de la rentabilité économique. En effet, dans la plupart des pays membres, la protection des données est un droit fondamental garanti par la constitution. Il ne s'agit donc pas ici uniquement de rentabilité économique, mais aussi de respect des obligations constitutionnelles de la part de l'Etat et de l'économie.

L'utilité de mettre en œuvre la biométrie (dont font partie les procédés d'identification basés sur les profils d'ADN) fera également l'objet d'une analyse. L'introduction d'un NIP (numéro d'identification personnel) sera également examinée. Enfin, outre l'identification dans le cadre de la lutte contre le terrorisme, les travaux porteront sur le contrôle éventuel des mouvements de population.

11.4 Autres thèmes

11.4.1 Conférence internationale des commissaires à la protection des données

La XXIV[ème] Conférence internationale des commissaires à la protection des données s'est déroulée à Cardiff du 9 au 11 septembre 2002. Elle réunissait des délégations provenant de 40 Etats de la planète. La Conférence a permis de faire le point sur les développements technologiques et de renforcer les contacts entre les commissaires à la protection des données et les responsables de traitement, notamment d'entreprises transnationales.

La Conférence a débuté par la séance réservée aux commissaires à la protection des données. Elle a permis de faire le point sur les développements intervenus depuis les événements tragiques du 11 septembre 2001. Dans la plupart des Etats, l'accent a été mis sur la lutte contre le terrorisme et le blanchiment d'argent. Plusieurs commissaires ont rappelé que toutes mesures restreignant les libertés des citoyens qui n'étaient pas nécessaires constituaient une victoire pour le terrorisme. Il est impératif de démontrer la nécessité d'une mesure et d'examiner si elle peut résoudre le problème posé (respect du principe de proportionnalité). Les commissaires se montrent également très prudents quant à l'introduction de mesures d'identification biométrique. Ainsi, lorsqu'elles sont introduites à des fins d'identification sur un document d'identité, il n'est pas nécessaire de les enregistrer dans une banque de données centralisée. La vérification d'identité peut se faire à partir du document. Enfin, il est important que les mesures envisagées fassent l'objet d'un débat démocratique et ne soit pas le seul fait des exécutifs. Les commissaires à la protection des données ont également eu un échange de vue sur les domaines qui les occupent en priorité. Plusieurs commissaires ont signalé une augmentation constante des plaintes en relation avec l'utilisation d'Internet. La mondialisation de l'Internet ne rend pas facile les investigations et il est nécessaire de renforcer les campagnes de sensibilisation auprès des internautes. Le spam constitue un autre sujet de préoccupation et les autorités de protection doivent faire face à une avalanche de plaintes. La vidéosurveillance, la surveillance sur le lieu de travail, la génétique, la rétention des données de trafic dans le secteur des télécommunications font également l'objet d'une large attention.

La deuxième partie de la Conférence était ouverte aux représentants des administrations, de l'industrie, des services et autres milieux intéressés. La Conférence avait pour thème général «Les droits à l'information au 21[e] siècle – une démythification». Elle a permis de se pencher sur les enjeux de l'accès à l'information et de la protec-

tion des données. C'est ainsi que les participants ont pu s'interroger sur les obstacles éventuels que les principes de la protection des données pourraient faire peser sur la marche des affaires des administrations ou des entreprises, notamment en empêchant la communication de renseignements. Il est apparu ainsi important d'avoir une approche proactive des problèmes et d'évaluer les avantages et les désavantages de l'accès ou du non-accès à l'information en considérant tous les acteurs, y compris les personnes concernées. Le respect de la vie privée n'est ainsi pas un obstacle à l'administration en ligne, mais il est indispensable de mettre en place un système qui garantisse le respect de la vie privée. Dans ce contexte, la technologie offre des possibilités de protéger les données personnelles tout en permettant l'échange d'informations. Le droit à l'anonymat est essentiel dans le système de la protection de la vie privée. Les personnes ne devraient en règle générale s'identifier que lorsque la connaissance de leur identité par une administration ou une entreprise est essentielle à une transaction particulière. La Conférence s'est aussi interrogée sur le rôle des autorités de protection des données dans un monde globalisé, sur l'apport de l'autoréglementation et sur la relation entre la protection des données et les libertés d'information et d'expression.

12. Le Préposé fédéral à la protection des données

12.1 Séance d'information de la Sous-commission 2 de la Commission des finances du Conseil national auprès du PFPD en septembre 2002

Nous avons reçu le 6 septembre 2002 la visite de la Sous-commission 2 de la Commission des finances du Conseil national. Celle-ci s'est particulièrement intéressée à notre organisation, à nos activités ainsi qu'aux difficultés inhérentes à nos ressources et moyens insuffisants. La Sous-commission a constaté notre sous-dotation en personnel et notre impossibilité à accomplir les tâches légales qui nous sont confiées. Lors de sa session d'hiver, le Conseil national a décidé que cette problématique devrait être débattue lors du traitement en 2003 de la révision partielle de la loi fédérale sur la protection des données.

Lors de la conférence de presse du 1er juillet 2002 pour la publication de notre 9ème rapport d'activités, nous avons lancé un appel sur le manque de ressources auquel nous sommes confrontés pour l'accomplissement de nos tâches légales. Souhaitant obtenir de plus amples informations sur cette problématique, la Sous-commission 2 de la Commission des finances du Conseil national, dans le cadre de ses discussions relatives à l'élaboration du budget de la Confédération pour 2003, a procédé le 6 septembre 2002 à une visite auprès de notre Secrétariat permanent. Au cours de

cette visite, nous avons dressé un bilan de nos activités et présenté nos perspectives à venir. La Sous-commission s'est intéressée en particulier à notre organisation, aux tâches légales qui nous sont confiées, à l'augmentation croissante de nos activités ainsi qu'aux difficultés inhérentes à nos ressources insuffisantes.

Questionnés sur les moyens dont nous disposons pour l'accomplissement de nos tâches légales, nous avons expliqué que le Préposé fédéral à la protection des données dispose d'un Secrétariat permanent de 16,2 postes. Avec cet effectif, nous sommes chargés de veiller à l'application des dispositions du droit fédéral de la protection des données par les organes fédéraux et les personnes privées. A cette fin, nous pouvons établir les faits d'office ou à la demande de tiers et le cas échéant recommander de modifier ou de cesser le traitement. Nos tâches relèvent du conseil, du contrôle, de la législation et de l'information. Nous avons signalé que notre effectif actuel ne nous permet ni d'accomplir l'ensemble des tâches légales qui nous sont confiées, en particulier sous l'angle du contrôle, ni de faire face aux nouveaux développements technologiques.

Sur la base de ces explications, la Sous-commission a souhaité recevoir des exemples plus concrets de certaines de nos activités et des moyens engagés pour les effectuer. Nous avons expliqué que par exemple dans le domaine de la sécurité et de la lutte contre le terrorisme, on assiste à un renforcement des moyens des autorités fédérales qui débouchent sur une augmentation des traitements de données par des organes fédéraux. Cette tendance s'est encore accentuée par la nécessité de renforcer la sécurité intérieure et la lutte contre la criminalité suite aux événements de septembre 2001. Cet accroissement des tâches fédérales dans le domaine de la police et de la poursuite pénale est suivi d'une forte augmentation des effectifs notamment de l'Office fédéral de la police. Or ces mesures ne sont pas accompagnées d'un renforcement de nos moyens pour effectuer les contrôles nécessaires et accompagner le développement des projets informatiques.

Nous avons également sensibilisé la Sous-commission au fait que dans le secteur de la santé, l'explosion des coûts rend nécessaire une rationalisation du traitement des données de santé et une meilleure coordination des activités entre les différents acteurs de la santé. Ces développements ne doivent toutefois pas se faire aux détriments des droits des patients et des assurés et notamment de leur droit au respect de la vie privée. En outre, cette évolution implique une sollicitation accrue de notre part, notamment dans l'accompagnement de projets (carte de santé, dossier électronique du patient, échange de données entre fournisseurs de soins et assurances, etc.). Faute de moyens, nombreux sont les projets qui ne peuvent être examinés et qui ne reçoivent pas de réponses. En particulier, nous n'avons jamais été en mesure d'exercer nos tâches légales en matière de recherche médicale et notamment de

surveiller le respect des charges qui grèvent les autorisations délivrées par la Commission d'experts du secret professionnel en matière de recherche médicale.

Enfin, nous avons attiré l'attention de la Sous-commission sur des projets liés aux développements des technologies de l'information et en particulier le e-gouvernement (guichet virtuel et vote électronique), pour lequel de gros moyens ont été débloqués dans l'administration fédérale sans augmentation de nos ressources pour répondre aux demandes d'accompagnent de cet important projet. Tel est également le cas pour l'introduction du numéro d'identification personnel et de la carte d'identité électronique, l'harmonisation des registres administratifs, ou encore des projets du secteur privé notamment dans le domaine du commerce électronique, du e-banking, du e-learning ou du e-marketing (problème épineux du spamming).

Se déclarant étonnés des moyens limités qui nous sont octroyés par rapport aux tâches confiées, des membres de la Sous-commission ont demandé quelles démarches avaient été entreprises pour remédier à cette situation insatisfaisante. Nous avons expliqué que nous avons mis en place un certain nombre de mesures de rationalisation et notamment introduit un système de gestion des dossiers («EDSB-Office») permettant une planification et un meilleur suivi des priorités et des objectifs fixés. Malgré ces mesures, notre effectif est resté insuffisant pour faire face à l'ensemble de nos tâches légales. Ce constat était d'ailleurs déjà celui de la Commission de gestion du Conseil des Etats qui dans son rapport du 19 novembre 1998 sur la mise en place des liaisons online dans le domaine de la police relevait: «La Commission de gestion partage l'avis du Préposé fédéral à la protection des données, qui estime qu'il manque de moyens, et notamment de personnel, pour exercer les contrôles dont il est chargé. Ce problème avait déjà été soulevé dans le cadre de l'inspection sur l'introduction de l'informatique dans l'administration fédérale, et force est de constater qu'il est toujours d'actualité» (FF 1999 5226). Dans sa réponse du 1er mars 1999 à une question ordinaire Widmer «Protection des données» (98.1185), le Conseil fédéral a reconnu le bien-fondé des observations de la Commission de gestion concernant le manque de ressources du PFPD: «Le Conseil fédéral est conscient de ce problème et est prêt à examiner dans quelle mesure les moyens du PFPD pourraient être renforcés, toutefois dans les limites imposées par la planification des dépenses en personnel» (CN BO 1999 I 594). Ces constatations n'ont toutefois toujours pas débouché sur un renforcement de nos forces nous permettant d'accomplir les tâches légales qui nous sont confiées.

En comparaison avec les autorités de protection des données d'autres pays, le Secrétariat permanent du PFPD, avec ses 16,2 postes, est moins bien loti que ses collègues à l'étranger pour des tâches pourtant similaires. Ainsi par exemple, les Pays-Bas ont un effectif de 56 personnes. La Belgique, la Grèce et le Danemark ont respectivement

un effectif de 22, 24 et 26 personnes. L'autorité suédoise dispose d'une équipe de 42 personnes. La République slovaque a un effectif de quelques 80 personnes. En Italie, en Pologne et en Tchéquie, chaque autorité nationale de protection des données est dotée de 100 personnes. Le Préposé fédéral allemand, qui n'est compétent que pour le secteur public fédéral, dispose d'un secrétariat de 63 personnes; à cela s'ajoute l'effectif des autorités de protection des données des Länder qui comptent chacune entre 30 et 40 personnes. La Commission nationale de l'Informatique et des Libertés en France (17 commissaires) dispose d'un secrétariat de 76 personnes. Selon une enquête des commissaires européens à la protection des données, on compte pour l'ensemble des 15 Etats membres de l'Union européenne, 586 postes à plein temps dévolus aux autorités de protection des données, soit une moyenne de 40 postes par Etat.

A l'issue de cette visite, les membres de la Sous-commission ont relevé la sous dotation du Secrétariat permanent du PFPD en personnel et son impossibilité d'accomplir ses tâches légales dans ces conditions. Cette problématique a été portée devant la Commission des finances du Conseil national puis débattue le 26 novembre 2002 à la session d'hiver du Conseil national dans le cadre des débats concernant le budget 2003 de la Confédération. A cette occasion il a été décidé de ne pas anticiper le débat sur cet objet dès lors que cette discussion serait abordée lors du traitement dans le courant 2003 de la révision partielle de la loi fédérale sur la protection des données dans le cadre de laquelle le Conseil fédéral pourra être amené à solliciter des moyens supplémentaires. Le Conseil fédéral a finalement décidé que la question des ressources sera traitée dans le cadre des discussions budgétaires 2004 et non lors de la révision de la LPD.

12.2 Neuvième Conférence suisse des Commissaires à la protection des données

La neuvième Conférence suisse des Commissaires à la protection des données a eu lieu le 22 novembre 2002 à Zoug. Les discussions ont essentiellement porté sur l'identificateur fédéral de personnes, les procédés biométriques de reconnaissance automatique des visages ainsi que les développements dans le domaine de la sécurité intérieure.

L'administration fédérale, sous la direction de l'Office fédéral de la statistique, envisage d'introduire un système d'identificateurs de personnes numérotant de manière uniforme l'ensemble de la population de Suisse. Le fait d'utiliser un identificateur univoque de personnes permettrait de rationaliser la gestion des registres administratifs. La discussion entre les représentants de l'Office fédéral de la statistique ainsi

que de l'Office fédéral de la justice et le préposé fédéral à la protection des données a néanmoins montré que la sphère privée des individus s'en trouverait considérablement atteinte car ce système permettrait d'associer et d'exploiter des informations provenant de domaines administratifs les plus divers. Le danger d'abus s'en trouverait en outre augmenté. Pour des raisons relevant de la protection de la sphère privée, la constitution portugaise par exemple interdit la numérotation univoque de la population. Le préposé fédéral à la protection des données a souligné qu'un identificateur fédéral de personnes ne peut être introduit sans que cela soit précédé d'un large débat démocratique (voir à ce sujet paragraphe 1.2.1).

Toujours au cours de cette conférence, le représentant d'une entreprise allemande de logiciels a présenté les procédés de reconnaissance automatique des visages. Des procédés similaires d'autres fabricants seront du reste mis en œuvre prochainement à l'aéroport de Kloten pour le contrôle des voyageurs entrant en Suisse. Il est apparemment possible de concevoir ces techniques dans le respect de la protection des données car le logiciel permet de rendre méconnaissables les visages enregistrés. Un décryptage peut avoir lieu ultérieurement sur ordre du juge.

De l'avis du landammann zougois et directeur de la police, il serait inutile que le législateur donne à la police des instruments de contrôle supplémentaires; il estime par ailleurs qu'il conviendrait d'exploiter à fond les moyens actuellement disponibles et rejette l'idée d'un système de collecte des informations couvrant l'ensemble du pays, tel que le projette actuellement le gouvernement américain sur son territoire. «Un Etat libéral ne peut promettre la sécurité totale à ses habitantes et ses habitants qu'en échange de son âme». A ses yeux, nous vivons dans une société à risques et nous ne pouvons pas les éliminer totalement.

12.3 Les publications du PFPD – Nouvelles parutions

- Bulletin d'information du PFPD 2/2002
- Bulletin d'information du PFPD 1/2003

Le site du PFPD

Notre site Internet est régulièrement complété et mis à jour. Ainsi, nous venons de créer deux nouvelles rubriques. Dans la rubrique «Questions & Réponses», nous répondons aux questions que le public nous pose fréquemment à propos de la protection des données; les «Questions & Réponses» sont classées par domaine et sont périodiquement mises à jour. Dans la rubrique «Publications » figure une nouvelle

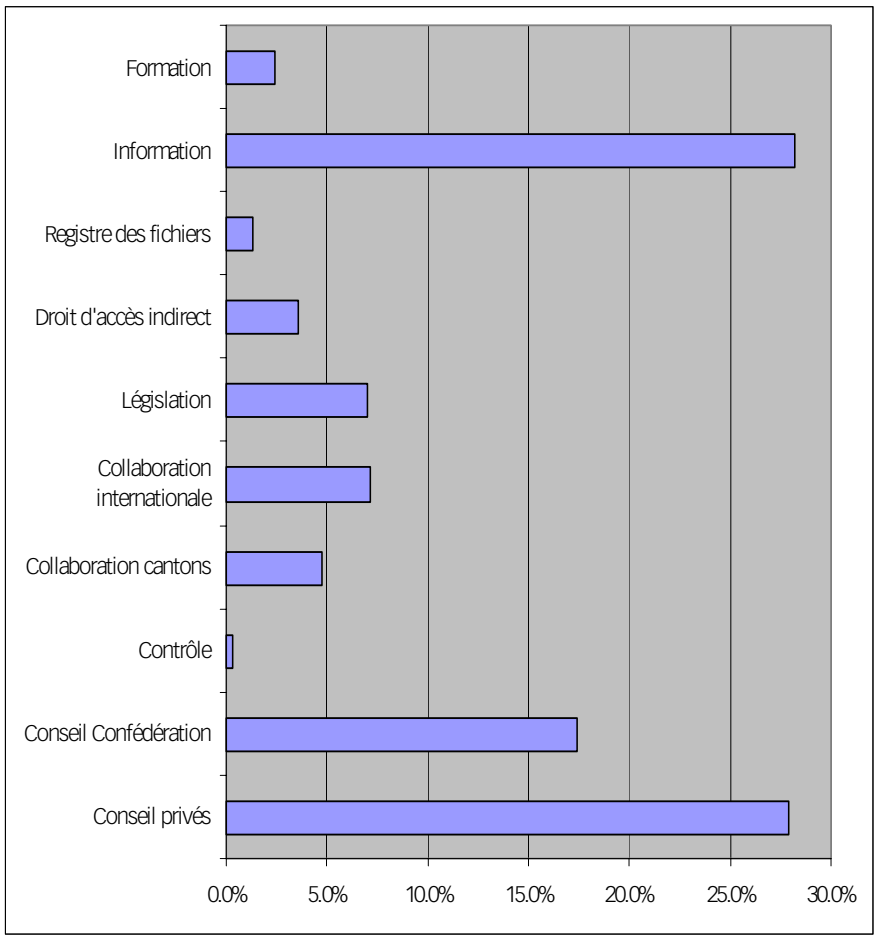
«sous-rubrique» contenant des articles publiés par les collaborateurs du PFPD dans des journaux et revues spécialisés («Publications/Presse spécialisée»). Par ailleurs, nous publierons bientôt, sous la rubrique «Lois & Commentaires», une liste des textes de loi ayant trait à la protection des données. Il est à noter que la rubrique «Thèmes», qui réunit des textes relatifs à des thèmes donnés, est elle aussi régulièrement complétée.

De nouvelles informations dans les domaines suivants:

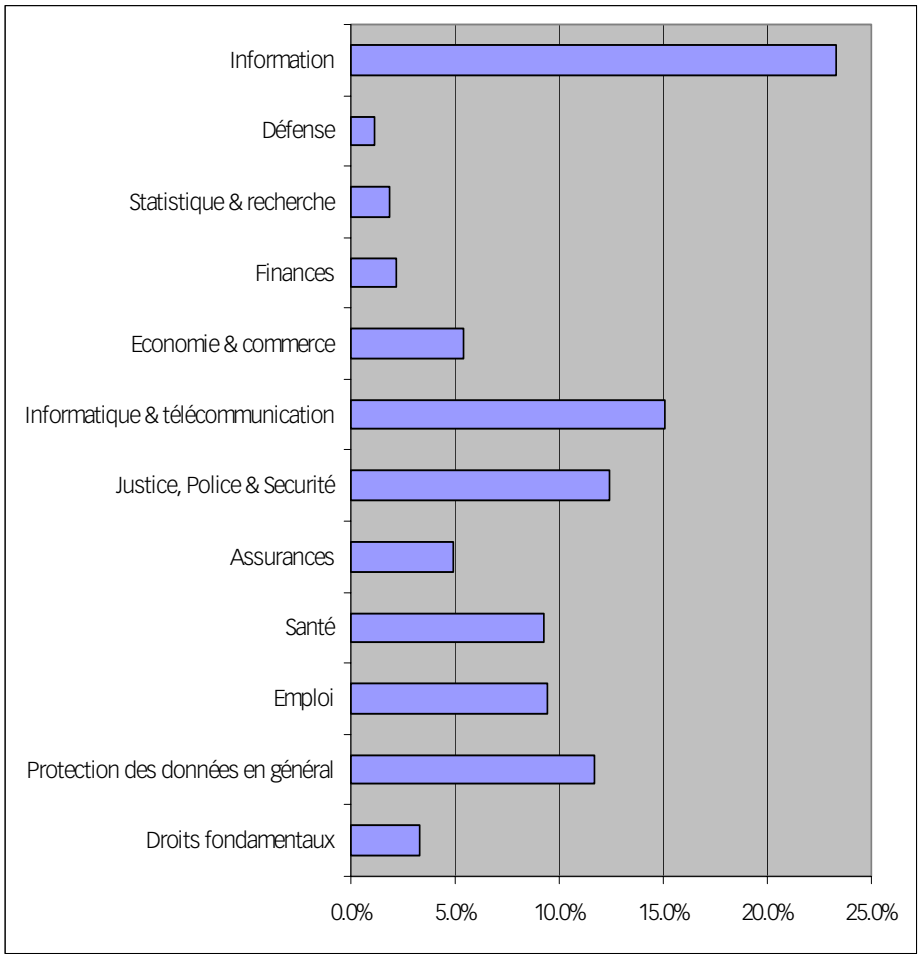
- Tests génétiques de paternité
  (http://www.edsb.ch/f/themen/weitere/index.htm)
- Télécommunications : Questions & Réponses
  (http://www.edsb.ch/f/fragen/index.htm)
- Santé : Questions & Réponses
  (http://www.edsb.ch/f/fragen/index.htm)

12.4 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2002 au 31 mars 2003

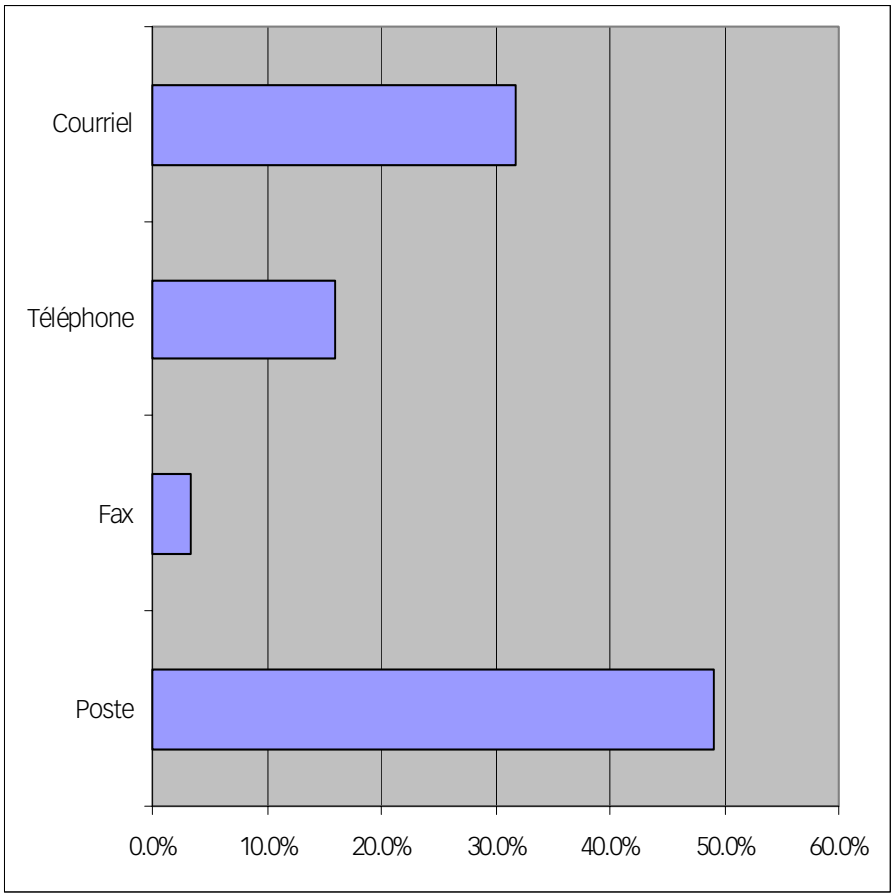
Charge de travail par tâches



Charge de travail par domaine



Provenance des demandes



12.5 Composition du Secrétariat du Préposé fédéral à la protection des données

Préposé fédéral à la protection des données:	Thür Hanspeter, Fürsprecher
Suppléant:	Walter Jean-Philippe, dr en droit
Secrétariat:	
Chef:	Walter Jean-Philippe, dr en droit
Suppléant:	Buntschu Marc, lic. en droit
Service d'information et de presse:	Menna Daniel, lic. phil. Tsiraktsopoulos Kosmas, lic. en droit
Service juridique:	7 personnes
Service informatique:	5 personnes
Chancellerie:	3 personnes

13. Annexes

13.1 Clause minimale de protection des données dans les conditions générales des fournisseurs de services de télécommunication

1.1 Dans le cadre du traitement des données personnelles nécessaires à la conclusion et à l'exécution du contrat, FST X peut échanger des données avec des autorités publiques et des entreprises privées chargées du recouvrement de créance et du renseignement de crédit afin de vérifier sa solvabilité et en cas d'incidents de paiement.

1.2 Lorsqu'une prestation est accomplie conjointement par FST X et des tiers ou que le client sollicite des prestations de tiers via le réseau de FST X, cette dernière peut communiquer des données relatives au client à des tiers, dans la mesure où cette communication est nécessaire à la fourniture et la facturation de telles prestations.

1.3 Dans les limites fixées par la législation sur la protection des données, en garantissant en particulier un niveau de protection équivalent au droit suisse, FST X peut communiquer des données à l'étranger dans le cadre de la gestion du trafic international (Roaming), de la fourniture d'informations (call center) et de l'établissement des factures.

2.1 Le client, à moins qu'il ne s'y soit expressément opposé, accepte que FST X traite

version 1 les données personnelles suivantes… [par ex. nom, prénom, adresse…]

version 2 des données personnelles (la liste des données peut être obtenue à l'adresse…)

pour développer des prestations personnalisées et établir des offres particulières (publicité personnalisée).

2.2 Le client, à moins qu'il ne s'y soit expressément opposé, accepte également que les données susmentionnées puissent être communiquées pour les mêmes finalités aux partenaires commerciaux de FST X,

version 1 à savoir…

version 2 (la liste des partenaires peut être obtenue à l'adresse…)

Remarques:

Dans le cadre du droit d'opposition (cf. chiffre 2.1 et 2.2 ci-dessus), nous recommandons aux FST de prévoir soit dans le contrat même soit dans un formulaire séparé une rubrique spécifique. Par exemple:

- Je m'oppose à ce que *FST X* traite mes données personnelles pour développer des prestations personnalisées ou établir des offres particulières (publicité personnalisée).
- Je m'oppose à ce que *FST X* communique mes données personnelles pour les mêmes finalités à ses partenaires commerciaux.

13.2 Exemples de questions et réponses dans le domaine des télécommunications

Suis-je obligé de figurer dans les annuaires de télécommunication?

Non, depuis 1998, vous pouvez décider de figurer ou non dans les annuaires. Vous pouvez également choisir les données qui seront inscrites dans les annuaires. Cependant le choix des données qui figureront dans les annuaires est fortement limité. En effet, toute inscription se compose au minimum des éléments suivants:

1. nom et prénom ou raison sociale
2. adresse complète
3. rubrique sous laquelle l'abonné a décidé d'apparaître
4. son numéro de téléphone (numéro E.164)
5. signe distinctif « pas de messages publicitaires et interdiction de communiquer des données à des fins de prospections publicitaire directe ».

Puis-je renoncer à recevoir une facture détaillée?

Lorsqu'il s'agit d'un raccordement utilisé par plusieurs personnes (par ex. par une famille), vous aimeriez peut-être pouvoir renoncer à recevoir une facture détaillée pour éviter que le destinataire de la facture puisse voir quels sont les numéros qui ont été appelés car ceci peut être délicat (cabinets de médecin, d'avocats ou centres de conseils).

Vous avez le droit de recevoir la facture sans les détails. Adressez-vous pour cela à votre fournisseur. Il établira votre facture à l'avenir sans les données détaillées. Certains prestataires offrent également la possibilité de recevoir une facture détaillée dans laquelle les numéros appelés ne sont pas imprimés en entier. Cette variante vous permet néanmoins de vérifier l'exactitude de la facture tout en protégeant la vie privée des utilisateurs du raccordement. Demandez à votre fournisseur de services de télécommunication s'il offre cette possibilité.

J'ai l'impression que mes communications téléphoniques sont écoutées par des tiers. Que puis-je faire?

Si vous avez des indices sérieux que des tiers non autorisés écoutent vos conversations téléphoniques, vous pouvez déposer plainte en vertu de l'article 179bis CP (écoute et enregistrement de conversations entre d'autres personnes).

Votre fournisseur de services de télécommunication vous informe sur les risques d'écoute et d'ingérence qu'entraîne l'utilisation de ses services. Il vous offre ou indique des moyens adéquats permettant d'éliminer ces risques. [Art. 64 OST]

13.3 La décision du DETEC concernant les formules de réexpédition de la Poste et la mise à jour des adresses

Voir paragraphe 13.3 de la partie en langue allemande

13.4 Disposition standard de protection des données dans les accords de réadmission et de transit

1. Les données personnelles nécessaires pour l'exécution du présent accord sont traitées et protégées conformément aux législations sur la protection des données en vigueur dans chacune des parties contractantes et [aux dispositions des conventions internationales applicables en la matière auxquelles les parties contractantes sont liées].

2. Dans ce cadre, les données personnelles à communiquer concerneront exclusivement les données personnelles relatives à la personne à réadmettre et éventuellement celles des membres de sa famille (nom, prénom, le cas échéant nom antérieur, surnom ou pseudonymes, noms d'emprunt, date et lieu de naissance, sexe, et nationalités antérieure et actuelle); la carte d'identité ou le passeport; les autres données nécessaires à l'identification de la personne à réadmettre ainsi que les lieux de séjour et les itinéraires.

3. Les données personnelles ne peuvent être traitées que par les autorités compétentes pour l'exécution du présent accord et aux fins prévues par celui-ci. La partie contractante qui transmet les données est tenue de s'assurer de leur exactitude ainsi que de la nécessité et de l'adéquation au but poursuivi par la communication. S'il s'avère que des données inexactes ont été transmises ou que la transmission était illicite, le destinataire doit en être avisé immédiatement. Il est tenu de procéder à la rectification ou à la destruction des données en cause. Toute transmission ultérieure à d'autres autorités doit recevoir au préalable l'autorisation de l'autorité qui les a communiquées. Les données personnelles transmises ne seront conservées qu'aussi longtemps que l'exige le but dans lequel elles ont été communiquées.

4. Chacune des parties contractantes informe l'autre partie contractante, à sa demande, de l'utilisation des données personnelles transmises [et des résultats ainsi obtenus]. A sa demande la personne concernée sera renseignée sur les informations existant à son sujet et sur le mode d'utilisation prévu.

5. Les deux parties contractantes sont tenues d'inscrire dans leurs dossiers la transmission et la réception des données personnelles et de protéger efficacement les

données personnelles transmises contre l'accès non autorisé, leur usage abusif et la communication illicite. [Chaque partie contractante charge un organe indépendant approprié de contrôler le traitement et l'utilisation de ces données.]

13.5 Rapport du groupe AGX concernant le système RAI/RUG à l'attention du Bureau du DSB+CPD.CH

I. Généralités

1. Notre groupe de travail est formé des membres suivants : BL, FR, ZH, BE et PFPD. FR en assume la présidence.

2. Notre groupe de travail a été chargé d'examiner et de répondre, le cas échéant, à la question de savoir si le système RAI/RUG est admissible du point de vue de la protection des données.

3. Notre groupe a effectué les démarches suivantes :

   Il a tenu 5 séances. L'une de ces séances a été consacrée à une visite du home St. Johann à Bâle, une autre à une rencontre avec quatre représentants de VASOS et du Neuer Panther Club (Mmes Ruth Banderet, Alice Liber, MM. Ernst Widmer et Hansruedi Sigg) et une à une information de la part du Dr. Markus Anliker, Q-Sys. Le groupe AGX a encore tenu une séance avec notre collègue Jean-Louis Wanner, préposé à la protection des données BS qui avait donné un avis officiel sur ce système dans son canton.

   Le groupe a d'autre part reçu de la documentation sur d'autres systèmes utilisés par des homes en Suisse (BESA, grille élaborée par le médecin cantonal de FR).

4. Notre groupe a décidé, faute de moyens, d'une part, de ne pas faire d'examen des autres systèmes utilisés en Suisse et, d'autre part, de se contenter d'une analyse générale du présent système, ce d'autant plus qu'il faudrait procéder à l'examen comparatif des dispositions légales cantonales. Le groupe AGX estime que s'il fallait entrer dans un examen plus circonstancié, le Bureau devrait alors donner un mandat que l'on pourrait évaluer à un mois de travail à plein temps.

   Ce rapport a été soumis à notre collègue de BS et tient compte des ses remarques.

5. Préalablement, le groupe tient à signaler qu'il s'est trouvé face à une question fondamentale de savoir si le traitement des résidents et résidentes dans des homes au moyen d'une saisie systématique des moindres détails de la personne, de ses agissements et de ses comportements est encore compatible avec les droits de la personnalité. Le groupe cependant s'est limité à l'examen des questions relevant de la protection des données.

1. Que veut dire RAI/RUG ? C'est le RESIDENT ASSESSMENT INSTRUMENT/RESSOURCE UTILIZATION GROUP C'est un système développé aux Etats-Unis et distribué en Suisse par la firme Q-SYS SA, Saint-Gall. La partie RAI comprend un questionnaire appelé Minimum Data Set (MDS) qui sert à évaluer les besoins de chaque résident et résidente de home, par une description systématique de ses forces et difficultés. Cela devrait servir de base à des soins et accompagnement orientés vers les besoins du résident et de la résidente.

   Remarque : le but principal du système selon le Dr. Anliker (Q-SYS) est l'amélioration de la qualité pour les soins de longue durée.

   Le module additionnel RUG sert à une tarification différenciée, par exemple en 12 catégories.

   Remarque : de l'avis du groupe AGX, le classement des résidents est la raison principale de l'utilisation du système en pratique et non l'amélioration de la qualité; à Bâle-Ville, le but est aussi de contrôler la qualité et par là, dans des cas d'espèce, d'améliorer les prestations.

   Le système Q-SYS fait voir les principales fonctions suivantes du système ÚRAI/RUG

   (voir aussi http://www.qsys.ch>RAI/RUG):

- MDS : évaluation de la résidente et du résident et documentation (MDS sert de point de départ pour les autres buts)
- planification des soins (aide à la clarification)
- management des ressources (Case Mix, planification des postes)
- management de la qualité (indicateurs, mesure des outcome)
- tarifs/financement (groupe de dépenses pour les soins)

   De façon générale, le système comporte 250 questions (MDS) (cf. annexe 1) en principe obligatoires; le canton de Bâle-Ville a cependant obtenu un traitement particulier réduisant les questions obligatoires à quelque 210 questions, les autres étant facultatives*. Le système permet de classer les résidents selon une échelle de 12 catégories, chacune comptant encore des échelons (à signaler que le système BAK, utilisé précédemment par le canton de BS notamment, comporte 4 catégories).

   Les questions sont réparties comme il suit : d'abord, il y a une partie avec des données administratives (par exemple, le numéro AVS, la date de naissance) mais

aussi des données démographiques (formation professionnelle, domicile précédent, langue) et des questions sur les habitudes de vie. Ensuite, diverses capacités sont examinées (cognitives, visuelles, corporelles, continence…). Le questionnaire continue par les maladies et prend en considération l'état nutritionnel, l'état de la peau etc. Les activités quotidiennes sont répertoriées, ainsi que la médication, les mesures et traitements particuliers pris la semaine précédente. Le questionnaire se termine par les thérapies suivies et la capacité de se déplacer.

Les questions facultatives à BS sont celles figurant sur les trois premières pages, à savoir celles qui donnent des informations sur la personne, son histoire personnelle et ses habitudes. Les données démographiques ne sont pas significatives pour les soins.

Remarque : de la discussion avec le Dr. Anliker il ressort que les données démographiques ne seront pas utilisées pour les statistiques. De l'avis du groupe AGX, elles ne devraient dès lors pas du tout être exportées. Le système devra être installé de telle façon que seules les données nécessaires sous une forme complètement anonymisée pourront être exportées. Le home n'a pas le droit de transmettre directement la page 11 du questionnaire portant sur le diagnostic des maladies.

En résumé, ces 250 questions portent sur des données d'identification, médicales, des habitudes et comportements sociaux.

2. L'examen effectué nous amène à faire les remarques suivantes :

2.1 Bases légales : art. 104a al. 2 de la loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMaL) qui renvoie aux art. 49 et 50 LAMaL (cf. annexes 2). La feuille d'informations pour les résidents des homes cite les fondements juridiques suivants : les bases légales pour la constatation de données sont les art. 25, 32 et 33 de la loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMaL), l'art. 33 de l'ordonnance du 27 juin 1995 sur l'assurance-maladie (OAMaL) et les art. 7 et 8 de l'ordonnance du 29 septembre 1995 sur les prestations dans l'assurance obligatoire des soins en cas de maladie (OPAS).

2.2 Principes généraux :

Des informations à notre disposition, il est ressorti ce qui suit.

2.2.1 Il apparaît que ce système poursuit plusieurs buts, à savoir la qualité des soins et la gestion du home concerné, la classification des résidents et des résidentes visant à recevoir des subventions étatiques, le remboursement correspondant par les assurances, des statistiques concernant et destinées en principe au home concerné.

2.2.2 D'autres buts paraissent également visés ou possibles, notamment l'amélioration de la qualité des prestations, la comparaison entre les homes intéressant plus particulièrement les pouvoirs publics (subventions), le tout devant peser vers le bas sur les coûts des homes, aussi bien pour les assurances que pour les pouvoirs publics.

2.2.3 Ces buts, après examen des bases légales, paraissent être couverts par les dispositions de la LAMaL. En revanche, la question de savoir si ces buts sont véritablement en connexité au sens de l'art. 4 al. 3 LPD et des dispositions cantonales correspondantes (par exemple l'art. 5 de la loi sur la protection des données fribourgeoise) nous paraît problématique. Les buts ne sont pas forcément clairs et compatibles entre eux. La meilleure gestion des coûts va-t-elle de pair avec l'amélioration de la qualité ? Tous les buts doivent-ils être couverts par un seul système, par ex. le RAI-RUG ? La relation entre le Cardex et le système RAI/RUG reste à clarifier de façon à profiter des informations déjà disponibles dans le Cardex. Il faut aussi relever que, selon certains utilisateurs, le système engendre une charge considérable lors de son introduction et de sa gestion. Ici les responsables pour le système RAI/RUG souligneront

Certainement que cette combinaison des buts est justement la condition pour une bonne qualité des résultats. De l'avis du groupe AGX, il est inadmissible de récolter des données pour plusieurs usages, bien que ceux-ci aient un fondement juridique et que l'utilité des informations soit donnée pour tous les buts ou qu'il s'ensuive seulement un traitement limité approprié.

Le système doit être installé d'une façon telle que pour chaque champ de données il soit déterminé dans quel but il sera utilisé et qu'un exploitation selon le but ne soit possible qu'avec le champ de données défini au préalable.

En outre il faut partir d'un but principal : c'est la documentation sur les résidentes et les résidents ainsi que la tarification et le financement. Les données nécessaires à cette fin doivent être enregistrées. Les autres buts (planification, management de la qualité) sont des buts dérivés et doivent se contenter en premier lieu des données qui sont disponibles.

2.2.4 En ce qui concerne le principe de la bonne foi, nous pouvons relever d'une part que l'information du résident et de la résidente (respectivement de la famille et des proches) paraît en général lacunaire, voire considérée comme impraticable du fait de la complexité des questionnaires et d'autre part, qu'un consentement de la personne concernée ne peut dans la plupart des cas pas

être considéré comme „ éclairé „ ni donné librement puisque le risque est de ne pas pouvoir obtenir alors de remboursement de la part de l'assurance ou au pire de ne pas obtenir de place dans un home du tout. Le système est déjà opaque pour l'utilisateur (le home) et à plus forte raison pour le résident du home.

2.2.5 Le questionnaire est très complet (cf. annexe 1), voire à la limite perfectionniste. Les questions se rapportent à des données sensibles, sur la santé, sur la sphère privée, voire intime. L'ensemble donne un véritable profil de la personnalité. En l'état des informations, nous ne sommes pas persuadés de la nécessité de toutes ces questions pour chaque cas individuel traité par les homes. Le principe d'économie des données est totalement ignoré. Bien plus, nous estimons que le système ne respecte pas le principe de proportionnalité. Par ex. les informations sur la formation professionnelle passée (partie AB), la fréquentation régulière d'une église ou la consommation au moins une fois par semaine d'une boisson alcoolisée (partie AC) ou encore la mauvaise humeur le matin (partie E) en passant par les activités spirituelles/religieuses (partie N) ne sont pas nécessaires à la réalisation des buts du système RAI-RUG. De plus, répondre aux questions est obligatoire ; le système ne permet pas de continuer à l'utiliser sans donner chaque fois la réponse correspondant à la question.

2.3 Communication

Selon les informations, les données personnalisées devraient rester dans le home. Néanmoins, l'élaboration de statistiques est une des prestations que l'entreprise Q-Sys fournit sur demande. Les informations devraient être fournies à Q-Sys de façon parfaitement anonymisée, ce qui n'est pas le cas selon nos constatations. D'une part, les homes ne reçoivent aucune directive sur la façon de livrer leurs données, d'autre part, elle risquent de ne plus avoir le choix de les fournir ou non s'il devait s'avérer que les autorités publiques devaient en décider ainsi ou si les assureurs devaient en être également les destinataires.

Les points sur lesquels notre groupe a pu d'ores et déjà constater des problèmes sont les suivants : Comment les questionnaires doivent-ils être anonymisés (si l'année de naissance subsiste, s'il s'agit de maladies rares, de petits homes, etc. l'anonymat ne peut pas être assuré) ? De plus, selon le principe de proportionnalité, ne devraient être communiquées que les parties du questionnaire qui sont utilisables à des fins statistiques, ce qui n'est pas le cas des 250 questions. Si des parties du questionnaire sont facultatives, elles ne devraient pas être transmises à des tiers.

Finalement, il faut considérer que le home est soumis au secret de fonction, voire médical, ce qui oblige à ne fournir que des données anonymisées ou à obtenir auparavant la levée du secret.

2.4 Sur le plan technique

- Du point de vue de la conservation et de la destruction des informations, nous avons constaté que le système ne permet pas d'effacer des données. Il n'offre que la possibilité d'indiquer si une personne est décédée ou a quitté l'établissement. En outre, le système conserve indéfiniment les données ce qui ne respecte pas les dispositions en matière d'archivage.

- Quant à la sécurité et à la protection de la personnalité, nous avons remarqué que des données figuraient sans protection sur des ordinateurs (Access DB). Quant à l'exportation des données, ces dernières ne sont pas anonymisées et leur protection est défectueuse. Un accès planifié ou involontaire à des données sensibles, en l'état actuel des moyens technologiques, ne peut pas être exclu. De plus, la documentation du système est mauvaise. Il manque des informations sur les exigences de sécurité auxquelles le système devrait satisfaire et à quelles conditions; de plus, il n'existe pas de concept de protection des données.

- L'informaticien de notre groupe n'a pas pu se faire une idée de la façon dont le système parvient à la classification par manque d'informations.

III. Conclusions

Notre groupe est parvenu aux conclusions suivantes :

1. Il y a actuellement un développement des systèmes de traitement des résidents et des résidentes des homes, qui prend de nouvelles proportions. La collecte et la sécurité des données, la communication et la conservation des informations, de même que l'anonymisation, sont les problèmes posés par ces nouveaux systèmes en liaison avec l'obligation de secret.

2. D'une part, les enjeux économiques sont importants. (développement du système par Q-SYS) ; d'autre part, les intervenants (Etat, assurances) visent à faire baisser les coûts. Nous sommes conscients des intérêts en jeu, mais ils doivent prendre en compte les droits fondamentaux, surtout lorsqu'il s'agit des droits d'une tranche de population qui a besoin d'une protection particulière.

3. Les assureurs exercent actuellement déjà une forte pression sur certains homes (notamment dans le canton FR) pour obtenir les informations personnelles complètes permettant de classifier les résidents et les résidentes. Avec un système aussi perfectionné, on peut pronostiquer sans grand risque de se tromper que les

assureurs vont s'intéresser de plus près encore à obtenir les informations pour pouvoir vérifier si la classification est exacte et si la gestion du home est satisfaisante. A notre avis, des bases légales claires autorisant la communication systématique des données personnelles font défaut actuellement.

4. Le système est en grande partie opaque pour les résidentes et les résidents des homes.

5. Les données seront systématiquement enregistrées, indépendamment des besoins de soins de la résidente ou du résident. Cela conduit à une acquisition non conforme à la proportionnalité de données en réserve. Même si on admet une récolte systématique de certaines informations, celle-ci doit se limiter à une quantité raisonnable.

6. En l'état, le groupe AGX propose d'en rester à une approche succinte. Cela signifie que nous visons principalement deux buts :

- éliminer les défauts

- réduire le nombre des questions obligatoires

Au nom du groupe AGX
Dominique Nouveau Stoffel
Présidente

Fribourg, 17 juillet 2002/12 novembre 2002/DNS

Liste des adaptations nécessaires à apporter au système RAI/RUG

La liste ci-après contient des adaptations que le Groupe de travail santé (AGX) soutient et considère selon les informations en sa possession comme un minimum à apporter au système RAI/RUG. Sont réservées d'autres adaptations nécessaires qui découlent du droit cantonal.

A. Collecte des données personnelles conformément à son but

1. Limiter la récolte des données personnelles à une quantité raisonnable: déterminer et justifier le besoin en données personnelles au strict nécessaire selon le but prévu: planification des soins et financement (classement selon une échelle en catégories).
2. Veiller à ce que d'éventuels autres buts suivent bien l'objectif principal pour lequel les données personnelles sont collectées.
3. Les données doivent être récoltées seulement pour les objectifs poursuivis et non pour d'autres usages que permettrait le système.
4. Du point de vue technique, le système doit être organisé, de façon à ce que chaque champ de donnée fixe à quel but la donnée va servir. L'exploitation des données ne peut être effectuée que dans le but prévu.

B. Minimum Data Set (MDS)

1. En regard de l'exigence de limiter la collecte des données personnelles au strict nécessaire, le MDS doit être réduit à une quantité raisonnable de données: le moins possible de questions et contrôle du détail de chaque question.
2. Le nombre de questions obligatoires doit absolument être réduit au minimum. La réponse aux autres questions doit être facultative.
3. On doit pouvoir reconnaître si la question posée est obligatoire ou facultative.
4. Techniquement, le système doit être organisé de façon à ce qu'on puisse laisser des questions sans réponse.

C. Exploitation des données à des fins de statistiques

1. Fixer les données nécessaires à des fins de statistiques.
2. Le système doit être organisé techniquement, de façon à ce que seules les données nécessaires à des fins de statistiques soient transmises (par ex. pas de transmission de données démographiques, pas de transmission de diagnostics des patients).

3. Les données ne peuvent être transmises par les homes que complètement anonymisées. L'anonymisation doit correspondre à des exigences minimales définies.

D. Sécurité des données

1. Les données ne doivent pas être sauvegardées non protégées. Elles doivent être protégées par les moyens techniques actuels à disposition (par ex. droit d'accès différencié, application de technologies et de chiffrements pour la mémorisation et la communication des données, signature numérique). Les mesures de protection sont d'autant plus élevées, qu'il s'agit de données sensibles.

E. Amélioration de la transparence

1. On doit pouvoir facilement comprendre quelles sont les données utilisées, comment, où et combien de temps elles sont conservées dans le système.
2. Le système doit permettre l'archivage des données.

Le système doit permettre d'effacer les données dont on n'a plus besoin.

Fixer un délai maximal d'archivage.

F. Documentation

1. Préparer une information écrite à l'attention des résidents et résidentes des homes et de leurs proches qui les renseignera sur le traitement des données et de le comprendre.
2. Elaborer un concept de protection des données qui décrira la mise en application des principes généraux de la protection des données.

Berne, 20 août 2002

13.6 Déclaration des commissaires européens à la protection des données

Déclaration des commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff (9-11 septembre 2002), relative à la conservation systématique et obligatoire des donnés de trafic des télécommunications.

Les commissaires européens à la protection des données ont constaté avec inquiétude que le troisième pilier de l'Union européenne examine actuellement des propositions qui auraient pour conséquence la conservation systématique et obligatoire des données de trafic relatives à l'usage de tout moyen de télécommunication (ex : détails concernant la durée et le lieu des appels, les numéros utilisés pour téléphoner, envoyer un fax, un e-mail et les données relatives aux usages d'Internet) pour une durée d'un an ou plus, afin d'en permettre l'accès aux autorités chargées de vérifier l'application effective de la loi.

Les commissaires européens à la protection des données ont des doutes importants quant à la légitimité et la légalité de telles mesures. Ils tiennent également à attirer l'attention sur les coûts excessifs de telles mesures pour l'industrie des télécommunications et de l'Internet, ainsi que sur l'absence de telles dispositions aux Etats Unis.

Les commissaires européens à la protection des données ont souligné à plusieurs reprises qu'une telle mesure constituerait une infraction aux droits fondamentaux garantis aux personnes par l'article 8 de la convention européenne des droits de l'homme, tel que précisé par la Cour européenne des droits de l'homme (voir l'avis 4/2001 du groupe institué par l'article 29 de la directive 95/46/CE, et la déclaration de Stockholm, avril 2000).

La protection des données de trafic dans les télécommunications est maintenant prévue dans la directive 2002/8/CE du Parlement européen et du Conseil concernant la vie privée et les communications électroniques (Journal Officiel L 201/37), qui précise que le traitement des données de trafic est en principe autorisé pour la facturation et le paiement des interconnexions. Après un très long et très explicite débat, il a été établi selon l'article 15 (1) de la directive que la conservation des données de trafic à des fins policières doit remplir des conditions strictes : dans chaque cas la conservation des données doit être prévue pour une période limitée et constituer une mesure nécessaire, appropriée et proportionnelle dans une société démocratique.

Lorsque des données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus. La conservation systématique de tout type de données de trafic

pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable.

Les commissaires européens à la protection des données espèrent que le groupe de travail de l'article 29 sera consulté sur les mesure qui pourraient être envisagées au sein du troisième pilier avant qu'elles ne soient adoptées.

13.7 Recommandations du PFPD

13.7.1 Recommandation concernant les centres fitness

Voir paragraphe 13.7.1 de la partie en langue allemande.

13.7.2 Recommandation concernant les tests de paternité

Recommandation

conformément à

l'art. 29, al. 3,

de la loi fédérale du 19 juin 1992

sur la protection des données (LPD)

concernant

le test de paternité

commercialisé par

l'entreprise X

I. Le Préposé fédéral à la protection des données constate les faits suivants:

1. L'entreprise X a informé le Préposé fédéral à la protection des données (PFPD) qu'elle envisageait de commercialiser un test de paternité en collaboration avec des pharmacies et a demandé son avis concernant les questions qui pourraient se poser en matière de protection des données.

2. Le PFPD s'est prononcé sur la problématique de la protection des données en relation avec des tests de paternité effectué en dehors d'une procédure administrative. Il a constaté notamment qu'un test de paternité représente une analyse génétique qui ne peut se faire qu'avec le consentement écrit de toutes les personnes concernées. En outre, le consentement n'est valable que si la personne concernée agit de plein gré et après avoir reçu toutes les informations nécessaires pour l'évaluation des conséquences possibles du test. Afin d'éviter que des tests de paternité soient effectués de manière cachée, il est indispensable que des mesures appropriées soient prises pour contrôler la validité des consentements recueillis.

3. Après avoir appris par des tiers que l'entreprise X va mettre sur le marché le test de paternité à partir du mois de décembre 2002, le PFPD s'est adressé à l'entreprise X en lui demandant des explications détaillées sur la procédure de distribution et, en particulier, sur la mise en pratique de ses remarques

4. Par la suite, l'entreprise X a informé le PFPD sur la procédure prévue. Il en sort qu'un contrat de mandat (qui n'a pas été soumis au PFPD) doit être signé par les personnes concernées (père, mère, enfant). Les enfants sont considérés capable de discernement à partir de l'âge de 14 ans. Pour les enfants de moins de 14 ans « Le(s) parent(s), détenteur(s) de l'autorité parentale, s'engage(nt), par leur(sa) signature(s), à consentir au test de paternité ». En outre, « en cas de conflit d'intérêts entre l'un des parents et l'enfant, les parents doivent s'adresser à l'autorité tutélaire de leur canton de domicile, qui pourra désigner un curateur pour déterminer le consentement de l'enfant. »

5. Pour le PFPD restent ouvertes des questions fondamentales concernant la licéité des consentements et, par conséquent, la façon légale ou non dont sont recueillis les échantillons biologiques :

- Comment et par qui les personnes concernées sont-elles informées sur le test et ses conséquences possibles?
- Comment vérifie-t-on l'identité des personnes concernées et l'authenticité de leurs signatures?
- Selon quels critères a-t-on fixé la limite de 14 ans pour la capacité de discernement?
- Comment vérifie-t-on le discernement de l'enfant concerné concrètement?
- Comment assure-t-on qu'un éventuel conflit d'intérêt entre les parents et l'enfant soit reconnu?
- Comment assure-t-on une procédure unitaire auprès des distributeurs (pharmaciens ou autres)?

II. Considérants:

1. Dans la mesure où ils nécessitent le traitement de données personnelles, les tests de paternité proposés par des entreprises privées tombent sous le coup de la LPD (art. 2, al. 1, let. a, LPD).

2. Le profil d'ADN utilisé pour l'établissement de la filiation contient des informations propres à la personne concernée, informations qui sont mises en évidence par une analyse génétique des échantillons prélevés sur cette personne.

3. Les profils d'ADN et les résultats de l'analyse sont des données personnelles sensibles au sens de l'art. 3, let. c, LPD. Les échantillons (dans le cas présent, il s'agit d'échantillons de salive) remis par la personne qui demande le test contiennent des informations spécifiques qui sont analysées lors du test de paternité.

4. Conformément à l'art. 29, le PFPD établit, dans le secteur privé, les faits d'office ou à la demande de tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un grand nombre de personnes (erreur de système) [art. 29, al. 1, let.a, LPD]. Si le traitement des données est contraire à certaines dispositions de la protection des données, le PFPD peut, en vertu de l'art. 29, al. 3, LPD, recommander de modifier ou de cesser le traitement des données ou d'y renoncer.

5. Un test de paternité – dont la première étape consiste à prélever des échantillons biologiques – constitue un traitement de données personnelles au sens de la LPD : un motif justificatif doit donc être invoqué. L'art. 13, al. 1, LPD prévoit comme motifs justificatifs possibles le consentement de la personne lésée, un intérêt prépondérant privé ou public, ou une loi. Dans le cas d'un test de paternité effectué librement, c'est-à-dire en dehors d'une procédure administrative, seul le consentement de la personne concernée entre en ligne de compte. L'exécution d'un tel test n'est permise qu'avec le consentement explicite de toutes les personnes concernées.

6. Du point de vue de la protection des données, un consentement doit remplir certaines conditions. La loi ne contient pas de dispositions particulières sur la forme du consentement. Mais comme il s'agit, dans le cas présent, de données particulièrement sensibles, il est indispensable que la personne concernée donne son consentement **par écrit**, consentement qui, pour être valable, doit en outre avoir été donné **de plein gré**. Si la personne concernée souhaite un délai de réflexion, celui-ci doit lui être accordé. De plus, pour que la personne prenne vraiment conscience de la portée de son accord (« consentement **éclairé** »), il faut qu'elle soit informée des faits et des conséquences possibles. Un consentement éclairé suppose que la personne concernée ait reçu au préalable toutes les informations nécessaires pour pouvoir évaluer les conséquences possibles de son acte. Le devoir d'information revient, en premier lieu, à la société qui offre ses tests sur le marché.

7. Un test de paternité peut avoir d'importantes conséquences (notamment psychiques) pour toutes les personnes concernées et nécessiter que différentes décisions soient prises. Or, il est difficile d'imaginer qu'une personne peut vraiment apprécier la portée d'un tel test (en particulier les conséquences d'un résultat

que personne n'attendait) sans avoir été informée et conseillée par un spécialiste. La personne concernée doit en outre être informée du but et du déroulement du test à proprement parler, ainsi que du traitement des données et des mesures liées à la sécurité des données (transmission, sauvegarde et destruction des données, protection contre leur utilisation par des tiers, anonymisation, pseudonymisation, etc.).

8. Il faut préciser enfin que le consentement est **révocable** en tout temps de manière inconditionnelle et sans forme particulière. Si une personne révoque son consentement par oral ou par écrit et que l'analyse n'est pas encore commencée, celle-ci n'est pas effectuée ; les éventuels échantillons fournis sont détruits, de même que l'ensemble des données rassemblées dans le cadre du test de paternité.

9. Il faut donc préciser dans la clause de consentement que le consentement est donné librement, après avoir reçu toute l'information nécessaire et qu'il peut être révoqué en tout temps.

10. L'entreprise qui offre et effectue le test de paternité (ou le fait effectuer par des tiers) doit s'assurer que les échantillons ont été prélevés en toute licéité. Il est tout à fait fondamental, du point de vue de la protection des données, que les échantillons soient recueillis de façon licite. De ce fait, toute entreprise qui propose des tests de paternité est soumise à **une obligation particulière d'information et de contrôle**. Elle doit donc veiller à ce que la personne qui demande le test soit conseillée par des spécialistes, et que les consentements écrits des personnes concernées (le père présumé, la mère et l'enfant) qui lui sont remis par le mandataire, fassent l'objet d'un examen rigoureux.

11. Une entreprise ne peut pas reporter sur la personne qui demande le test la responsabilité de la validité des consentements recueillis. Sans un examen rigoureux des consentements donnés, il serait imaginable que des tests de paternité soient effectués « secrètement ». Or, il est interdit d'effectuer des tests de paternité sur la base d'échantillons qui ont été recueillis sans le consentement valable des personnes concernées. De tels tests constitueraient une violation grave des droits de la personnalité de l'enfant et du partenaire.

12. Eu égard à ces considérations, le PFPD est parvenu à la conclusion que la procédure prévue ne répond pas aux exigences posées par les dispositions de protection des données. Les droits de la personnalité des personnes concernées sont donc sérieusement menacés, puisque plusieurs conditions nécessaires à la validité du consentement ne sont pas remplies. Ainsi, par exemple, l'information des personnes concernées est insuffisante ; de plus, il n'y a pas d'examen rigoureux

de la validité des consentements écrits remis par la personne qui demande le test.

III. Sur la base de ces considérants, le Préposé fédéral à la protection des données recommande:

1. L'entreprise X renonce à diffuser le test de paternité jusqu'à ce que le traitement des données en question soit conforme aux conditions posées dans la LPD.

2. L'entreprise X s'engage à remplir son obligation d'informer ses clients de sorte que ceux-ci puissent donner leur consentement en connaissance de cause (« consentement éclairé »). L'entreprise X prend les mesures nécessaires pour que ses clients soient informés et conseillés par des spécialistes. Elle peut par exemple leur remettre un document détaillé élaboré par des spécialistes et leur demander la confirmation par écrit qu'ils ont lu le document. De plus, l'entreprise X met à la disposition de ses clients un spécialiste auquel ils peuvent adresser en tout temps, par oral ou par écrit, leurs éventuelles questions.

3. L'entreprise X modifie le contrat prévu, notamment la clause de consentement, en tenant dûment compte des points mentionnés dans les considérants.

4. L'entreprise X s'engage à remplir son obligation de contrôle en procédant à un examen rigoureux des consentements écrits qui lui sont remis par ses clients, par exemple en exigeant des copies de documents officiels, en téléphonant aux personnes qui ont donné leur consentement etc.

5. La validité des consentements écrits donnés par des personnes mineures capables de discernement doit être examinée avec un soin particulier. En cas de doute, l'entreprise X doit également recueillir le consentement du représentant légal de cette personne (c'est-à-dire celui des deux parents ou du parent qui s'en est vu confier la garde).

6. S'il y a des doutes concernant la licéité du prélèvement de l'échantillon, l'entreprise X ordonne un nouveau prélèvement, qu'elle effectue elle-même ou fait effectuer par un tiers qui est neutre.

7. L'entreprise X informe le PFPD de toutes les mesures prises en matière de protection et de sécurité des données dans le cadre du test de paternité.

8. L'entreprise X informe par écrit tous ses collaborateurs et auxiliaires du devoir de discrétion qui leur incombe en vertu de l'art. 35 LPD.

L'entreprise X communique au PFPD, dans les 10 jours qui suivent la date à laquelle elle reçoit la présente, si elle accepte ou non sa recommandation. Si elle la rejette ou ne la suit pas, le PFPD peut porter l'affaire devant la Commission fédérale de la protection des données.

La présente recommandation est notifiée à l'entreprise X par courrier recommandé avec accusé de réception.

LE PRÉPOSÉ FÉDÉRAL
À LA PROTECTION DES DONNÉES
Le Préposé:

Hanspeter Thür

13.7.3 Recommandation concernant le Spam

Voir paragraphe 13.7.3 de la partie en langue allemande