9. Tätigkeitsbericht 2001/2002

9ème Rapport d'activités 2001/2002

Eidgenössischer
Datenschutzbeauftragter

Préposé fédéral à la protection
des données

Rapport d'activités 2001/2002

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 2000 au 31 mars 2001.

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 a modifié de manière soudaine la discussion sur le rapport entre sécurité publique et protection de la personnalité. Depuis que deux avions ont réduit en cendres les deux tours du World Trade Center de New York, la discussion ne s'est pas affaiblie. Dans le monde entier, les thèmes les plus discutés actuellement sont la lutte contre le terrorisme et la question de la sécurité publique. Et au centre des débats surgit donc la question de savoir jusqu'où la protection des données peut aller face à cette menace. La question est légitime, étant donné que la protection des données n'agit pas isolément: elle doit continuellement peser les divers intérêts qui sont en jeu. C'est un défi que l'on doit accepter lorsqu'on s'engage pour la protection des données. C'est finalement la société qui doit décider le niveau de sécurité publique qu'elle désire et dans quelle mesure elle est prête pour cela à sacrifier une partie de la protection de la vie privée.

En notre qualité de responsables de la protection des données, nous devons pourtant accompagner ce processus et veiller à ce que les principes de la loi sur la protection des données, qui sont identiques à ceux d'un Etat de droit, ne soient pas perdus de vue. C'est la raison pour laquelle nous avons à maintes reprises indiqué qu'il fallait toujours analyser les raisons d'un fait avant de réagir et que seules des mesures proportionnelles et appropriées devaient être envisagées. Cela signifie que les mesures proposées doivent effectivement procurer plus de sécurité et qu'il doit être avéré que cet objectif ne peut pas être atteint moyennant une autre mesure qui serait moins radicale à l'encontre de l'individu.

A ce propos, deux points méritent d'être soulignés: un renforcement de la sécurité publique ne doit pas a priori être obtenu aux dépens de la protection de la personnalité. Si l'on constate par exemple que les attentats ont été fortement favorisés par l'insuffisance des contrôles effectués dans les aéroports des Etats-Unis, il n'y a pas d'objection du point de vue de la protection des données à renforcer ces contrôles car protection des données n'est synonyme ni de protection des coupables, ni de protection des terroristes.

Mais en même temps, il est nécessaire de retenir qu'une manière très rigoureuse de voir la sécurité peut détruire les fondements d'un Etat de droit. Nous devons toujours nous rappeler qu'une sécurité absolue n'existe pas. Notre civilisation occidentale devient de plus en plus vulnérable, plus le progrès technique avance. Les scientifiques et les intellectuels ont analysé ce phénomène de la «société à risque» déjà bien avant la date du 11 septembre. Ces dernières décennies, ce sont surtout les menaces liées à la production d'énergie nucléaire et aux processus chimiques et biochimiques qui ont été au centre de la discussion. Un facteur de risque supplémentaire qui a été introduit

est que les stratégies terroristes se servent également de ces risques techniques qui ont été créés par les humains. Ce qui est nouveau, c'est qu'entre-temps les terroristes sont effectivement prêts à user de ces moyens. Les théoriciens du risque avaient depuis longtemps prévu cette éventualité et nous avaient vainement mis en garde.

Comment faut-il faire face à un tel défi dans un Etat de droit? Se pourrait-il que l'effondrement des tours du World Trade Center soit en même temps l'effondrement de nos espoirs de faire un «usage civilisé» de nos menaces techniques modernes? La tentation en tout cas est grande que l'on ne débatte plus du sens des menaces qui ont été créées par la technique et de leurs alternatives éventuelles, mais que l'on se concentre à instaurer la sécurité en utilisant les immenses possibilités techniques disponibles aujourd'hui pour contrôler et surveiller les citoyens. Sécurité totale signifierait alors introduction d'immenses banques de données ADN combinées avec une investigation par recoupement, création de profils psychologiques, surveillance par vidéo et satellites à grande échelle, mise en relation de toutes les bases de données existantes et utilisation du système GPS (Global Positioning System) qui permet à tout moment de déterminer l'emplacement d'une personne. Il ne s'agit pas là d'une chimère issue d'un roman de science-fiction, mais bel et bien d'une vision d'horreur qui est réalisable avec les moyens techniques dont nous disposons de nos jours. Orwell a depuis longtemps été dépassé par les possibilités réelles! Pour éviter que cette horreur ne se transforme progressivement en réalité, nous devons conduire un débat ouvert avec des citoyens responsables qui sont conscients du fait qu'une sécurité totale nous mènerait droit au totalitarisme.

Ce débat sur les risques doit donc être élargi de manière radicale si nous ne voulons pas assister à une désagrégation de l'Etat de droit. Si ce processus est toujours rampant, c'est parce que des valeurs telles que démocratie, protection des données et droits à la liberté ne sont pas simplement présentes ou absentes; elles sont toujours plus ou moins présentes pour disparaître lorsqu'elles ne sont plus sollicitées ou défendues. Nous devons être conscients du fait que plus nous faisons évoluer nos moyens techniques (centrales nucléaires, manipulation génétique, technologies informatiques, Internet etc.), plus nous devenons vulnérables. Il y a une certaine probabilité que des catastrophes – pas seulement d'origine terroriste! – se produiront vraiment dans le cadre de ce qui est techniquement imaginable. Cela signifie que le débat sur le risque doit commencer avec la question de savoir quel est le progrès technique que la société est encore prête à accepter au vu de l'accroissement des menaces. Selon le principe, il n'est pas admissible de réaliser tout ce qui est techniquement faisable. Si ce débat sur le risque est limité au seul domaine de la lutte contre le terrorisme, nous oublions d'autres menaces pareillement dangereuses et nous nous berçons en fin de compte d'une image de sécurité trompeuse. L'exemple d'Internet nous démontre

combien cette discussion est délicate: personne n'aimerait vouloir se passer de ce moyen de communication d'une simplicité géniale. Des secteurs entiers de l'économie en vivent et il est utilisé quotidiennement, non seulement par des multinationales, mais également par des petites et moyennes entreprises. Si le soupçon existe actuellement qu'Osama bin Laden ait préparé et coordonné les attaques à l'aide d'Internet, on pourrait être tenté de contrer cette menace en soumettant tout trafic Internet à un contrôle extrêmement strict et en interdisant le cryptage des communications (comme le demandent les Etats-Unis). Mais ceci signifierait en même temps la fin d'Internet, car qui serait encore prêt à utiliser ce moyen de communication si nous devons nous attendre à ce que les services secrets puissent prendre connaissance à tout moment des messages que nous transmettons? Ceci illustre qu'il n'y a plus de réponses simples dans notre monde complexe. En fin de compte, force est de constater que nous vivons dans une société à risque (que nous approuvons régulièrement) et que nous devons en conséquence sciemment percevoir ces risques.

Mon prédécesseur Odilo Guntern – auquel je tiens à exprimer ici ma reconnaissance et mes remerciements pour l'excellent travail d'édification qu'il a effectué en qualité de premier Préposé fédéral à la protection des données – a rendu attentif en 1994 dans son premier rapport d'activités au fait qu'une des tâches du Préposé était de sensibiliser le public aux problèmes de la protection des données. Il a de manière remarquable réussi à atteindre cet objectif. Si cette institution jouit aujourd'hui d'une grande considération dans la population et qu'elle est quotidiennement sollicitée pour donner conseil ou prendre position, c'est à lui ainsi qu'à ses collaborateurs que le mérite en revient. Je poursuivrai ces efforts.

Actuellement pourtant, la sécurité intérieure semble refouler à l'arrière-plan tous les autres thèmes. Il y a cependant d'autres domaines dans lesquels des développements importants constituent un défi pour la protection des données. Dans le domaine de la santé publique, le dossier médical électronique se développe de plus en plus et crée ainsi des chances et des menaces pour la protection des données. Nous maintenons un contact étroit en accompagnant un projet avec lequel nous désirons montrer de manière exemplaire comment il est possible de tirer profit des chances tout en évitant les risques. La carte de santé est une autre nouveauté qui fait l'objet d'une discussion impliquant aussi les responsables de la protection des données.

Un débat important a lieu actuellement sur l'utilisation d'analyses ADN dans le cadre de procédures pénales. Dans quels cas un tel examen peut-il être effectué et qui peut finalement être enregistré dans une banque de données ADN et pour quelle durée?

Une importance non moindre revient à la révision actuellement en cours de la loi sur la protection des données. Elle nous procurera un renforcement important de la protec-

tion de la personnalité puisqu'elle prévoit que les citoyens devront automatiquement être informés lorsque des données sensibles les concernant sont traitées ou enregistrées. Personnellement, je souhaiterais que cette révision prévoie également un renforcement de la responsabilité propre des personnes qui sont chargées du traitement des données. La protection des données devrait de plus en plus être utilisée comme argument de vente et les consommateurs devraient donner la préférence aux entreprises et aux produits qui sont exemplaires en matière de protection des données. Dans le domaine de la protection de l'environnement, cette approche s'est imposée depuis longtemps déjà. Un produit peut obtenir une mention le caractérisant comme étant particulièrement respectueux de l'environnement ou une denrée alimentaire peut obtenir la mention «biologique». Ceci a permis, l'année passée, à une grande chaîne de distribution de réaliser un taux de croissance bien au-dessus de la moyenne. Nous devrions viser le même objectif dans le domaine de la protection des données. Quiconque est prêt à se soumettre à un audit en matière de protection des données, devrait recevoir un label de qualité qui lui permettrait de bénéficier d'un avantage compétitif sur le marché. Ceci présuppose deux choses: le législateur devrait en tenir compte dans la révision actuellement en cours et les consommateurs devraient de plus en plus préférer les entreprises et les produits qui prennent au sérieux la protection des données.

Hanspeter Thür

Répertoire des abréviations

AUPER	Système d'enregistrement automatisé des personnes
CIRCA	Communication & Information Resource Centre Administrator
CJPD	Groupe de projet sur la protection des données
CJPD-GTPJ	Groupe de travail sur la protection des données et les données policières et judiciaires en matière pénale
CP	Code pénal suisse
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
GEWA	Système de traitement de données en matière de lutte contre le blanchiment d'argent
IDA	Interexchange of Data between Administrations (Echange d'informations entre administrations publiques)
IPAS	Système informatisé de gestion et d'indexation de dossiers et de personnes
ISIS	Système de traitement de données relatives à la protection de l'Etat
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAMal	Loi fédérale sur l'assurance-maladie
LCA	Loi fédérale sur le contrat d'assurance
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
OCSP	Ordonnance sur les contrôles de sécurité relatifs aux personnes
OEC	Ordonnance sur l'état civil
OFP	Office fédéral de la police
PESEUS	Groupe de Projet - DFJP - Stratégie - UE - Suisse
PJF	Police judiciaire fédérale
RCE	Registre central des étrangers
RIPOL	Système de recherches informatisées de police
SAP	Service d'analyse et de prévention
SIRENE	Supplément d'Informations Requis à l'Entrée Nationale
SIS	Système d'Information Schengen

1. Droits fondamentaux

1.1. Cyberadministration (e-government)

Malgré l'imprécision qui entoure le terme «e-government», ce dernier se prête néanmoins à être utilisé pour désigner les projets de transformation de l'administration dont la réalisation comporte une part informatique importante. Au niveau fédéral, citons en particulier le projet de Guichet Virtuel ainsi que les efforts visant à permettre le Vote Électronique. Les deux projets visent des objectifs très ambitieux et soulèvent des questions importantes au niveau de la protection des données.

Guichet Virtuel

Selon la stratégie en matière de cyberadministration de la Confédération, «Guichet Virtuel» est un de ses projets clés stratégiques. Son but est de «permettre aux citoyens de s'adresser aux autorités pour leur soumettre les problèmes qui se posent au quotidien». Cette description à elle seule montre déjà que l'objectif et les limites du projet sont très ambitieux, mais qu'en même temps ils ont été définis de manière extrêmement vague. Pour pouvoir procéder à une appréciation concrète du projet du point de vue de la protection des données, il est cependant essentiel de savoir quels seront finalement les transactions qui pourront être effectuées à ce guichet virtuel. Ce ne sera que sur la base des ces informations qu'il sera possible d'évaluer quelles informations transiteront ou pourront transiter par ce guichet et donc de définir les mesures de sécurité qui devront être attribuées et appliquées aux diverses transactions.

Dans la mesure où nous avons pu accompagner le prototype, celui-ci ne présentait pas encore de fonctions utiles pouvant être appréciées du point de vue de la protection des données. Selon la stratégie de la Confédération en matière de cyberadministration, il est prévu à partir de 2002 de «créer un portail pour la communication et les transactions». Pour diverses catégories de communication ainsi que pour chaque type de transaction, des questions de sécurité de nature organisationnelle et technique vont se poser, couvrant les divers domaines de la sécurité des données. Il y a lieu de relever en particulier le choix du procédé prévu pour l'identification et l'authentification, de sa forme prévue ainsi que des procédés qui seront chargés de garantir la confidentialité, que ce soit celle des participants ou simplement du contenu de la communication. D'autre part, la question devra être posée pour chaque transaction de savoir dans quelle mesure il faudra assurer son caractère obligatoire ainsi que sa traçabilité. La mise en œuvre correcte dans tous les systèmes qui interagissent avec le Guichet Virtuel des droits d'accès (autorisations), qui semblent évidents dans

le monde non virtuel, ne se fera pas de manière simple dans un certain nombre de cas. Finalement, le passage aux transactions virtuelles pourrait engendrer des modifications de compétences et ceci soulèvera des questions qui vont bien au-delà de l'aspect purement technique.

-Vote électronique

Le «Rapport sur le vote électronique» du Conseil fédéral du 9 janvier 2002 définit le terme «vote électronique» comme la réunion de trois catégories de fonction assez différentes. La première, qui donne aux autorités la possibilité de «*fournir des informations sur les votations populaires et sur les élections, et ce, par voie électronique*» existe en principe aujourd'hui déjà, dans une mesure plus ou moins grande. La possibilité de «*signer les demandes de référendum ou les initiatives populaires par voie électronique*» par contre pose déjà des exigences plus élevées, étant donné qu'elle nécessite une vérification de l'authenticité des signatures électroniques et des autorisations de signer.

La troisième catégorie, la possibilité de «*voter par voie électronique (lors de votations populaires ou d'élections)*» est de loin la plus complexe et mérite d'être examinée de plus près. La raison principale de la complexité n'est pas l'exigence de continuer à proposer – en plus de la voie électronique – les voies traditionnelles de l'urne et du vote par correspondance. Le cœur de la complexité se situe au niveau du conflit d'intérêts entre l'exigence de l'anonymité lors de l'exercice du droit de vote (secret du vote) d'une part et la nécessité d'autre part de pouvoir retracer l'opération dans une certaine mesure. Les deux critères sont caractéristiques de votations et d'élections au sens traditionnel et donc certainement des attributs également requis dans le monde virtuel. Pour illustrer la traçabilité, nous citerons le cas fictif suivant qui s'est produit en l'an 2015: à la suite d'une votation, un groupement politique fait courir le bruit que la votation a été falsifiée ou, encore mieux, que c'est lui-même qui l'a falsifiée. Que faire dans un tel cas? Sans possibilité de retracer les faits, il n'est pas possible de prouver ou de réfuter quoi que ce soit. Quant à l'éventualité de répéter le vote, il s'agit d'une solution qui dans la majorité des cas est hors de question. On peut pourtant soutenir que le jour viendra ou la traçabilité ne sera plus nécessaire parce que la confiance en l'informatique sera si grande que plus personne n'envisagera sérieusement la possibilité d'une erreur ou d'une brèche de sécurité. On peut avoir des avis divergents sur la question, nous aimerions simplement rendre attentif au fait que des experts en informatique renommés considèrent aujourd'hui les projets de vote électronique comme trop dangereux pour la démocratie. Il existe bel et bien des méthodes basées sur des signatures numériques invisibles qui permettent de surmonter dans une certaine me-

sure le conflit existant entre l'anonymité et la traçabilité. Pourtant, même ces méthodes ne permettent pas d'éliminer la complexité, sans compter qu'elles sont d'autant plus difficiles à mettre en œuvre. C'est pourquoi nous regrettons que, bien que la question de la faisabilité soit mentionnée dans le titre du rapport sur le vote électronique, le projet en soi n'inclue aucun élément concernant cette question.

Ce qui importe en premier lieu du point de vue de la protection des données dans ce projet est de savoir ce qu'il est prévu de faire avec les registres des électeurs. Ne serait-ce que pour des questions de coût, nous proposons de ne pas entreprendre de démarches importantes avant qu'un modèle concret n'ait été présenté qui donne une réponse affirmative et pertinente à la question de la faisabilité d'exercer son droit de vote via un réseau. Une réponse positive limitée au cas de figure de la signature de référendums ou d'initiatives ne serait vraisemblablement pas une justification suffisante pour investir dans la transformation des registres des électeurs, étant donné que les signatures récoltées par voie électronique ne peuvent pas être comparées à celles qui ont été récoltées selon la méthode traditionnelle, tout simplement parce qu'elles sont «plus faciles à obtenir».

2. Protection des données – questions d'ordre général

2.1. Communication de données personnelles

2.1.1. Invitation à remettre un inventaire de logiciels

Afin de vérifier si les licences de logiciel nécessaires existent, Microsoft Suisse a envoyé une lettre à des entreprises, les invitant à lui fournir des indications sur les produits logiciels qu'elles utilisent. Le texte de la lettre ne montrait pas assez clairement le caractère entièrement facultatif de cette consultation. Suite à notre intervention, Microsoft a accepté d'envoyer une deuxième lettre aux entreprises concernées dans laquelle elle insisterait de manière plus claire sur le caractère facultatif de la réponse.

Nous avons été réellement submergés de demandes suite à une lettre envoyée par l'éditeur de logiciels Microsoft. En novembre 2001, Microsoft a effectué un publipostage adressé à des petites et moyennes entreprises (PME) portant le titre «Votre entreprise utilise-t-elle également des copies illégales de logiciel?». Dans cette lettre, l'éditeur de logiciel demande aux PME de l'aider dans la lutte contre le piratage de logiciels. Elle les invite pour cela à fournir des indications détaillées sur les produits Microsoft installés dans leur entreprise ou à confirmer qu'elles n'utilisent aucun logiciel Microsoft.

Nombre de destinataires – parmi eux également des entreprises qui n'utilisent absolument aucun logiciel Microsoft – n'ont pas bien su comment réagir et nous ont demandés s'il y avait une obligation de répondre à cette lettre et plus particulièrement de fournir à Microsoft un inventaire des logiciels. Nous leur avons répondu par la négative.

Comme le texte de la lettre n'est pas assez clair sur le fait qu'il est facultatif de répondre ou non, nous avons demandé à Microsoft de s'adresser une deuxième fois aux destinataires de la lettre et de mettre en évidence de manière claire le caractère facultatif de cette réponse. Microsoft nous a assuré qu'elle le ferait.

Si un éditeur de logiciel dispose d'éléments permettant de soupçonner qu'une personne contrevient aux dispositions légales en matière de droits d'auteur protégeant ses produits, il peut s'adresser aux autorités compétentes qui prendront les mesures adéquates.

Nous avons en outre rendu attentif les personnes qui nous ont contactés au fait qu'elles peuvent exercer leur droit d'accès, prévu par la loi sur la protection des données, afin de découvrir quelles données les concernant sont traitées par Microsoft.

2.1.2. Communication des adresses des actionnaires

Les données personnelles des actionnaires sont mises à la disposition du conseil d'administration d'une société anonyme pour que celui-ci soit à même d'accomplir ses tâches. Il porte la responsabilité d'un traitement des données conforme aux principes de la protection des données.

Le conseil d'administration d'une société anonyme œuvrant dans le secteur financier nous a consultés pour savoir si les actionnaires qui le désiraient étaient en droit de communiquer les adresses, inscrites au registre des actions, d'autres actionnaires.

Les statuts de la société prévoyaient que le conseil d'administration était tenu d'autoriser les actionnaires à consulter le registre des actions et à copier les noms et adresses de personnes figurant dans ce registre dans la mesure où l'on pouvait prouver que ces données étaient nécessaires pour contacter les personnes concernées par courrier à propos d'une affaire concernant la société.

Mentionnons un fait qui n'influe pas sur l'appréciation du cas: cette disposition statutaire avait été mise en place avant l'entrée en vigueur de la LPD. En tant que personne privée, la société anonyme est du reste tenue d'appliquer les dispositions de la LPD.

En vertu de la LPD, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. En achetant des actions nominatives, les acquéreurs acceptent également

les statuts (à l'exception des clauses contraires aux normes impératives du droit de la société anonyme). Ils donnent ainsi leur consentement au traitement des données au sens de la disposition statutaire mentionnée. Le conseil d'administration est donc non seulement habilité, mais aussi tenu de garantir aux actionnaires l'accès au registre des actions s'ils peuvent apporter la preuve qu'ils ont besoin des données en question pour contacter les autres actionnaires à propos d'une affaire concernant la société.

Quant à la forme que prendra la communication des adresses, le conseil d'administration doit aussi scrupuleusement respecter les statuts qui prévoient clairement que le conseil d'administration doit autoriser les actionnaires à consulter le registre des actions et à copier pour leur usage les noms et adresses de personnes inscrites. Sur ce point, le droit suisse de la société anonyme établit uniquement que la société est chargée de tenir un registre des actions. Il ne s'exprime toutefois pas sur la question de savoir sous quelle forme cette tenue doit avoir lieu. Aujourd'hui, l'opinion dominante veut que les registres des actions puissent être aussi informatisés. Nous avons recommandé au conseil d'administration de ne remettre aux personnes intéressées que des listes imprimées ou copiées sur papier et pas de supports de données électroniques conformément au principe de la proportionnalité. En outre, nous avons recommandé au conseil d'administration de demander aux personnes auxquelles ces listes d'adresses sont remises de garantir que celles-ci ne seront pas utilisées à d'autres fins (par ex. pour l'envoi de publicité). A ce propos, la fixation d'une peine conventionnelle peut procurer une garantie supplémentaire.

2.1.3. Protection des données lors de recherches généalogiques

Les recherches généalogiques nécessitent la consultation de nombreux documents privés ou officiels pour lesquels il faut s'adresser aux autorités compétentes des cantons et de la Confédération. Les règles régissant la consultation et la protection des données diffèrent selon que les documents à consulter proviennent des registres publics relatifs à des rapports juridiques de droit privé (par exemple les registres de l'état civil) ou qu'il s'agit d'autres documents officiels. Il faut déterminer en premier lieu si les recherches sont effectuées directement auprès des personnes concernées ou au contraire dans des documents officiels.

Recherches effectuées auprès des personnes directement concernées ou auprès de tiers

La règle fondamentale qui s'applique ici est que les données personnelles qui concernent des personnes en vie doivent toujours être recueillies directement auprès de ces personnes. Si des recherches généalogiques sont effectuées directement auprès

des personnes concernées ou de tiers (personnes apparentées ou connaissances), la loi sur la protection des données est applicable. Celle-ci prévoit que quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées (art. 12 al. 1 LPD ; RS 235.1). En outre, personne n'est en droit, sans motif justificatif, de traiter des données contre la volonté de la personne concernée (art. 12 al. 2 let. b LPD). L'art. 13. al. 1 LPD mentionne à titre de motifs justificatifs le consentement de l'intéressé, un intérêt prépondérant privé ou public, ou la loi.

Il découle de ce qui précède que tout traitement de données personnelles effectué dans le cadre de recherches généalogiques, tel que l'acquisition, la conservation ou la publication de données, nécessite le consentement explicite des personnes en vie. Il faut en outre veiller à ce que la publication de données personnelles concernant des défunts ne porte pas atteinte aux droits de la personnalité des descendants, dont le consentement doit, en règle générale, être obtenu.

Recherches dans les registres de l'état civil ou d'autres registres publics relatifs à des rapports juridiques de droit privé

La loi sur la protection des données ne s'applique pas aux registres publics relatifs aux rapports juridiques de droit privé (art. 2 al. 2 let. d LPD). Parmi ces registres figurent en particulier ceux de l'état civil, qui font le plus souvent l'objet de recherches généalogiques. Ceci ne signifie pas pour autant que les recherches généalogiques dans les registres de l'état civil s'opèrent sans règles de protection des données. La consultation de tels registres est réglementée par l'ordonnance sur l'état civil (OEC, RS 211.112.1). Cette ordonnance précise que les particuliers n'ont en principe pas le droit de consulter les registres de l'état civil. L'autorité cantonale de surveillance peut cependant autoriser la divulgation de données personnelles à des fins de recherche scientifique lorsque l'obtention de ces données auprès des personnes concernées est impossible ou ne peut manifestement pas être exigée (art. 29a al. 2 OEC). Cette autorisation est cependant toujours assortie de conditions visant à garantir la protection des données. Pour obtenir cette autorisation, il faut adresser une demande écrite et motivée à l'autorité de surveillance du canton où les recherches doivent être effectuées.

Si les données ainsi obtenues doivent par la suite figurer dans une chronique familiale et donc être portées à la connaissance de tiers, la loi sur la protection des données devient applicable et il y aura lieu d'obtenir le consentement des personnes concernées. Si ce consentement est refusé, les données en question doivent être immédiatement détruites.

En ce qui concerne les recherches dans d'autres documents publics et la communication de données par les organes de la Confédération, nous renvoyons les lecteurs au 2e Rapport d'activités 1994/95, p. 191.

2.2. Protection et sécurité des données

2.2.1. Toutes les étapes entre l'identification personnelle et l'anonymat

Depuis tout temps, l'Homme a pu choisir d'entrer en relation avec ses congénères en révélant franchement, en dissimulant plus ou moins habilement ou en taisant carrément son identité. Selon la nature de la relation, le partenaire peut accepter ce choix, demander une augmentation de l'identification, voire même renoncer à toute forme d'interaction en cas de refus de l'intéressé. Cette pratique prend une importance considérable à l'heure de la communication interpersonnelle, de la diffusion médiatique, du commerce électronique et de bien d'autres services offerts par Internet. Il est dès lors important de bien définir les différentes formes et usages des modes anonymes ou pseudonymes sous lesquels un individu peut se présenter.

L'*identité* est définie dans le dictionnaire Larousse comme *l'ensemble des données de fait et de droit (date et lieu de naissance, nom, prénom, filiation etc.) qui permettent d'individualiser quelqu'un*. Les données nécessaires dépendent logiquement de la grandeur du contexte dans lequel l'identification doit avoir lieu. Dans un cercle restreint (classe, amis, collègues), un seul élément de l'identité comme le prénom suffit en général à identifier chaque personne. Dans un cercle plus large (école, entreprise), plusieurs éléments comme le prénom, le nom et parfois la date de naissance peuvent devoir être combinés pour parvenir à identifier chacun. Ainsi définie, l'identité ne comporte aucune caractéristique permettant d'identifier physiquement un individu, si bien que les documents officiels d'identité comportent en outre des données anthropométriques comme la taille, la couleur des yeux et une photo-portrait.

L'*anonymisation* est définie comme le fait de modifier des données personnelles de telle sorte que les informations relatives à la situation personnelle ou matérielle ne puissent plus (ou bien ne puissent l'être qu'au prix d'efforts démesurés) être mises en corrélation avec une personne physique déterminée ou déterminable. Cette définition implique clairement que toutes les données d'identification personnelle doivent être éliminées, puisqu'un seul de ces éléments peut conduire à l'identification dans un contexte restreint. Cette contrainte dépend bien sûr du pouvoir discriminant de l'élément d'identification: l'indication du sexe est ainsi anodine, tandis que la date de naissance doit être anonymisée en année de naissance ou en âge de la personne. Il est toujours risqué de conserver le moindre élément d'identification en tablant sur la grandeur initiale du contexte d'anonymisation, car celui-ci peut évoluer (notamment diminuer!) au cours du temps. Reste le «faux» problème d'une information imperson-

nelle tellement spécifique qu'elle permet à un tiers bien renseigné d'identifier une personne qu'elle connaît déjà très intimement.

Cette forme d'*anonymat non traçable* ne permet aucun recoupement entre des données enregistrées provenant de la même personne physique. Les paiements en espèce, même effectués auprès du même créancier, font partie de cette catégorie. Il existe cependant une forme d'*anonymat «traçable»*, caractérisé par le fait qu'un identificateur anonyme inclus dans chaque enregistrement permet de relier les événements provenant de la même source, soit éventuellement de la même personne. Les cartes (et certaines cartes à puce) téléphoniques à prépaiement illustrent parfaitement cette forme d'anonymat.

Quelle que soit la forme d'anonymat, les données ne doivent faire l'objet d'aucune mesure particulière de protection, étant donné qu'elles ne sont pas personnelles ou personnalisables. La notion de «désanonymisation» est impropre, car une réidentification des personnes n'est techniquement possible que dans le cas où l'anonymisation est incorrecte ou imparfaite!

La *pseudonymisation* est définie comme le fait de modifier les données personnelles par une *règle de correspondance* de telle sorte qu'il ne soit plus possible de mettre les informations relatives à la situation personnelle ou matérielle en corrélation avec une personne physique, sans avoir la connaissance de cette règle ou sans y avoir recours. Les *données d'identification sont ainsi remplacées par* une désignation, appelée *un pseudonyme*, fournie par la règle de correspondance. L'objectif de cette opération est de ne pouvoir rétablir la correspondance univoque avec l'identité («dépseudonymiser») qu'en cas de besoin et sous réserve de respecter des conditions préalablement définies. La pseudonymisation offre ainsi un *anonymat relatif* par rapport à tous ceux qui ne peuvent dépseudonymiser, mais sa levée peut être réalisée, notamment lorsque la responsabilité de l'intéressé est engagée. Les pseudonymes ne doivent en outre pas être communs à plusieurs applications, car une mise en relation de données pseudonymisées provenant de plusieurs sources pourrait conduire à l'élaboration d'un profil individuel dont l'accumulation de traits caractéristiques permettrait trop aisément une réidentification abusive.

La *pseudonymisation mathématique* est fournie par une *fonction à sens unique* qui produit un pseudonyme abstrait à partir des données personnelles d'identification. Cette fonction, basée sur une méthode de chiffrement asymétrique qui garantit l'impossibilité de remonter à tout ou partie des données d'identification à partir d'un pseudonyme, doit en outre posséder la propriété non triviale de pratiquement exclure l'éventualité de produire un pseudonyme identique à partir de données d'identification de personnes distinctes. En théorie, la «dépseudonymisation» est pos-

sible par comparaison du pseudonyme cible avec l'ensemble des pseudonymes obtenus à partir des données d'identification de toutes les personnes d'un groupe (attaque par dictionnaire) dans lequel se trouve la personne recherchée. Comme cette opération n'est pas toujours réalisable en pratique, certains se risquent alors à parler de «pseudonymat anonyme», notion apparemment très proche de l'anonymat «traçable». Les pseudonymes à sens unique se prêtent ainsi très bien aux études statistiques longitudinales dans lesquelles des données personnelles saisies a posteriori sont regroupées avec des données existantes, sans qu'il soit nécessaire d'établir la correspondance avec la personne considérée.

La *pseudonymisation exogène* est réalisée par la création d'un *pseudonyme de référence*, choisi le plus indépendamment possible de l'identité avec laquelle il est relié exclusivement par une *table de correspondance.* Cette table constitue donc la seule possibilité pour réidentifier les personnes, si bien que son accessibilité conditionne entièrement la robustesse de la pseudonymisation. Elle peut par exemple être déposée auprès d'un ou plusieurs tiers de confiance, qui peuvent même se répartir les clés permettant de dépseudonymiser. Avec la technologie actuelle, la table de correspondance devrait à notre avis satisfaire aux exigences suivantes pour que la pseudonymisation puisse être qualifiée de robuste:

- seules des personnes accréditées et formellement authentifiées en assurent la gestion,
- la table est conservée uniquement sous une forme électronique chiffrée,
- la réidentification ne peut avoir lieu que sélectivement pour un pseudonyme donné (le pseudonyme pourrait même ne pas être mémorisé et jouer uniquement le rôle de clé symétrique de chiffrement-déchiffrement donnant accès à l'identité correspondante),
- une journalisation exhaustive des réidentifications avec motif justificatif est établie.

Lorsque la table de correspondance est *semi-publiquement accessible*, soit par exemple gérée par une institution s'engageant à la garder confidentielle (ex: numéro de carte de crédit), la sécurité repose exclusivement sur le sérieux avec lequel les employés, les débiteurs et la personne concernée traitent ces données. Il faut cependant reconnaître que les mesures de nature organisationnelle sont en règle générale moins efficaces que celles de nature technique (cf. exigences formulées ci-dessus).

Dans le cas où la table de correspondance serait par contre *publiquement accessible* (ex: listes blanche et verte de l'annuaire téléphonique), la pseudonymisation est si faible qu'on devrait plutôt parler d'*identification indirecte* des personnes.

La *pseudonymisation endogène* est réalisée par les *noms de plume*, qui sont des pseudonymes créés par la personne concernée et pour lesquels la correspondance avec son identité réelle reste ainsi entièrement sous son contrôle. La seule précaution utile est de s'assurer que le pseudonyme choisi n'est pas déjà utilisé par quelqu'un d'autre (vérification d'unicité). Ce type de pseudonymat convient entre autre très bien à un cadre d'études scientifiques qui visent à livrer des renseignements génériques sur des groupes de personnes précis, mais qui veulent aussi donner aux intéressés la possibilité de s'informer incognito sur leurs résultats individuels.

Pour conclure, on peut constater que les formes entre l'anonymat et l'identité sont multiples et subtiles. Chaque forme se prête spécialement bien à un type particulier de relation, si bien qu'une personne peut être amenée à utiliser à tour de rôle toutes les formes possibles. Pour un internaute, une telle gestion est indiscutablement très ardue et astreignante, si bien qu'une assistance par le biais d'un *protecteur d'identité* sera tôt ou tard nécessaire.

2.2.2. Bureau électronique

L'environnement bureautique mis à disposition des employés par l'employeur comprend de plus en plus souvent un gestionnaire de bureau électronique intégrant le traitement du courrier électronique et la fonction d'agenda électronique. Vu les nombreux enjeux en matière de protection des données, le courrier électronique fait l'objet d'un thème à part (voir ci-après). Si l'agenda électronique comprend traditionnellement un calendrier, un carnet d'adresses, un échéancier de tâches et un bloc-note, le bureau électronique offre en outre la possibilité d'activer un journal permettant le suivi des activités, d'archiver automatiquement les éléments jugés surannés, de partager les données du bureau avec certains collègues et même de les synchroniser avec des équipements portables ou carrément avec des serveurs Internet.

Bien qu'un mélange d'éléments professionnels et privés soit pratiquement inévitable, le bureau électronique est couramment aussi appelé un gestionnaire d'informations personnelles (PIM: Personal Information Manager). Cette appellation est révélatrice de la confusion qui règne entre la partie professionnelle de l'univers personnel de l'employé qui «appartient» à l'employeur et sa sphère privée qui ne cesse pas d'exister au moment où il franchit la porte de l'entreprise et qui doit rester protégée. Lorsque l'emploi nécessite une certaine mobilité et le poste de travail n'est pas transportable, l'employeur fournit parfois encore à l'employé un ordinateur de poche synchronisable avec le bureau électronique, ainsi qu'un téléphone cellulaire. Cette dissé-

mination des données ne va pas sans poser des problèmes de sécurité et de protection, autant pour l'employé que pour l'employeur. Ce dernier doit en tous les cas impérativement définir les conditions dans lesquelles un administrateur peut accéder aux conteneurs d'information du bureau électronique des employés, que ceux-ci se trouvent sur une unité de stockage d'un serveur d'entreprise, du poste de travail ou de l'ordinateur de poche de l'employé, aussi bien que sur un quelconque support de sauvegarde.

L'activation du *journal de suivi des activités* permet de conserver automatiquement une *trace chronologique de raccourcis* vers les messages, réunions et tâches associés à certains contacts, ainsi que vers certains types de documents bureautiques créés (textes, tableurs, présentations ou bases de données). Le journal peut de plus être complété par des entrées manuelles pour lesquelles un suivi est également souhaitable (ex: appels téléphoniques). Cette trace peut ainsi témoigner d'activités accomplies à une certaine époque, quand bien même les documents de base auraient par la suite été détruits! L'activation d'un tel journal doit donc être mûrement réfléchie, surtout si les raccourcis sont statiques et perdent le lien avec les éléments déplacés ultérieurement à des fins de classement. La liste des courriels en rapport avec chaque personne présente dans le carnet d'adresses peut en principe être dressée indépendamment du journal (onglet «Activités» de l'élément de type «Contact» correspondant), mais celle-ci est en principe inoffensive du fait qu'elle n'affiche que les messages encore présents dans les dossiers (y compris celui des éléments supprimés!) du bureau électronique.

L'*archivage automatique* des éléments surannés est possible de manière sélective pour chaque type de dossiers du bureau électronique et offre le choix entre l'archivage dans un dossier personnel et la suppression définitive. L'archivage offre l'avantage de décharger le bureau électronique de ses anciens éléments, tout en maintenant la possibilité de consulter les éléments archivés en cas de besoin. Cela peut évidemment créer un risque en matière de traçabilité d'informations disparues.

Lorsqu'une autorisation d'accès aux éléments professionnels doit être accordée à certains collègues, l'employé doit avoir la possibilité de *marquer distinctement ses éléments privés*, afin que leur contenu ne soit au moins pas rendu public (affichage grisé) ou mieux encore qu'aucune trace de leur existence ne soit dévoilée! Un rendez-vous hebdomadaire en soirée peut en effet donner lieu à diverses interprétations.

Du fait de la mobilité requise par certains emplois, du cumul possible d'emplois à temps partiel et de l'extension du télétravail, le bureau électronique de l'employé doit rester disponible quasiment en toute circonstance. Pour ce faire, il n'y a en fait que trois solutions techniques possibles:

- *permettre l'accès au bureau électronique d'entreprise depuis un réseau externe*, avec des risques liés à l'authentification de l'employé et à la confidentialité des données échangées que seule une infrastructure à clés publiques permet de véritablement maîtriser. L'accès peut ainsi être offert par le biais de passerelles WAP (Wireless Application Protocol) pour téléphones cellulaires ou alors de passerelles RAS (Remote Access Service) pour ordinateurs portables reliés au réseau téléphonique fixe (modem ou carte ISDN: Integrated Services Digital Network) ou directement au réseau téléphonique cellulaire (protocoles HSCSD: High Speed Circuit Switched Data ou GPRS: General Purpose Radio Service). La technologie des réseaux virtuels privés (VPN: Virtual Private Network) peut de surcroît être engagée pour assurer une sécurisation accrue des communications.

- *Synchroniser le bureau électronique avec un équipement personnel portable*, avec des risques liés au maintien de la confidentialité de données généralement assurée par des mots de passe d'accès ou plus efficacement par un cryptage des données. Par équipement personnel portable, il faut comprendre les ordinateurs portables (en mode autonome), les ordinateurs/organiseurs de poche et les téléphones cellulaires. A l'heure actuelle, seuls les ordinateurs portables disposent d'un système d'exploitation supportant un système de fichiers avec un niveau de cryptage élevé. Des extensions de cryptage plus ou moins robustes existent pour les ordinateurs de poche (palmtops et HPC: Handheld Personal Computers), qui sont en général plus performants que les assistants numériques personnels (PDA: Personal Digital Assistants), aussi appelés agendas électroniques ou organiseurs de poche. Le marché propose aujourd'hui déjà des équipements de poche qui combinent les services d'organisation personnelle et de téléphonie.

- *Synchroniser le bureau électronique avec un site Internet offrant ce genre de services*, avec des risques liés au niveau de confidentialité et de disponibilité des données assuré par le prestataire choisi. Certains prestataires offrent par exemple un service gratuit de synchronisation des données du calendrier, du carnet d'adresses et des tâches du bureau électronique, complété par des gestionnaires intégrés de courriels, de messages SMS, de télécopies, de messages vocaux et de fichiers partageables, parfois même accessibles depuis un téléphone cellulaire supportant le protocole WAP.

2.2.3. Courrier électronique

L'environnement bureautique mis à disposition des employés par l'employeur comprend traditionnellement un gestionnaire de courrier électronique, parfois intégré à un gestionnaire de bureau électronique. Les courriels véhiculent des informations, de nature professionnelle ou parfois privée, qui peuvent en outre être aussi bien internes à l'entreprise qu'en relation avec des partenaires externes. Leur protection doit donc faire l'objet d'une attention toute particulière, notamment grâce à des fonctionnalités souvent méconnues et sous-exploitées des gestionnaires de messagerie.

Il suffit par exemple d'utiliser le *champ «CCi»* (Copie Carbone invisible) plutôt que le champ «À» pour que les multiples destinataires du message aient l'impression d'avoir été adressés individuellement, c'est-à-dire qu'ils n'aient pas connaissance des adresses des autres destinataires choisis par l'expéditeur. Cette mesure convient très bien à des messages impersonnels (publicités, annonces.) adressés à un groupe de personnes ne se connaissant mutuellement peut-être pas, mais contrevient au principe fondamental de transparence lorsqu'elle est utilisée pour faire parvenir une *copie grise* à d'autres destinataires («CCi») que les destinataires principaux («À») et accessoires («CC»).

La demande *d'accusé de réception* et surtout celle de *confirmation de lecture* assure l'expéditeur de la non-répudiabilité d'un message effectivement transmis au destinataire et ouvert (donc en principe lu.) par ce celui-ci.

L'option de *délai d'envoi* permet de mettre un embargo effectif sur un message, tandis que celle de *date d'expiration* garantit la destruction automatique d'un message périmé, c'est-à-dire plus du tout d'actualité et dont la lecture n'aurait plus aucun intérêt.

La fonction de *rappel de message* permet de rattraper la divulgation accidentelle d'un message, à condition d'être utilisée avant que les destinataires n'en aient déjà pris connaissance.

Les *critères de diffusion* permettent en outre de caractériser chaque message envoyé quant à sa confidentialité (Normal, Personnel, Privé, Confidentiel). Les messages reçus avec l'attribut «Privé» peuvent ainsi rester invisibles pour les éventuels délégués (voir plus loin) ayant le droit de relever votre boîte aux lettres. Pour les messages reçus avec l'attribut «Confidentiel», il serait souhaitable que leur transfert soit conditionnel à une confirmation explicite de l'intention de propager l'information vers d'autres destinataires!

Pour la confidentialité, le *cryptage du contenu et des pièces jointes* (mode asymétrique dans une infrastructure à clés publiques) constitue indiscutablement la mesure la plus efficace. Le cryptage garantit en outre l'intégrité des données reçues, étant donné que la moindre modification (intentionnelle ou accidentelle) du message crypté conduit à l'impossibilité de son décryptage. Une *signature numérique ajoutée au message sortant* permet en outre au destinataire de vérifier l'authenticité de l'expéditeur.

Des *règles de gestion* peuvent en outre être définies de manière personnalisée, afin que les messages soient par exemple automatiquement vérifiés, assignés à certaines catégories (par ex. Privée), déplacés, supprimés, copiés ou encore transférés en fonction de critères portant sur leur contenu et/ou leurs données accessoires. Une liste des expéditeurs de *courrier indésirable (polluriels et autres pourriels)* peut même être définie.

En cas d'*absence du bureau*, il existe notamment la possibilité de définir une *réponse automatique aux messages entrants* pour renseigner les expéditeurs sur la durée de l'absence (la cause étant en principe parfaitement inutile!) et les coordonnées d'une personne de contact en cas d'urgence. Dans ce même cadre, il est en outre possible de définir un *transfert automatique des messages* reçus vers une adresse externe choisie, ce qui doit inciter à la plus grande prudence quant à la confidentialité des messages, potentiellement sensibles pour l'employeur comme pour l'employé, ainsi redirigés vers une boîte aux lettres accessible, donc vulnérabilisée, par Internet!

Il reste à aborder le problème crucial de la *conservation des messages* échangés. Bien que la pratique démontre un excès de conservatisme conduisant à la saturation fréquente des espaces de stockage, cela ne signifie pas pour autant que certains messages importants ne soient pas intempestivement détruits ou excessivement difficiles à retrouver. La solution passe par l'usage de *boîtes aux lettres de service non nominatives* (ex: info@firme.ch), ainsi que par des consignes strictes pour l'*enregistrement des messages dans le système de gestion des affaires* de l'entreprise.

Dans le cadre des *systèmes de gestion de courriels*, les messages font l'objet d'un pré-traitement automatique basé sur des règles d'entreprise (business rules) définies par l'employeur pour leur validation, catégorisation, «prioritisation», acheminement, conservation et archivage. Les employés ne reçoivent alors souvent qu'un jeton d'accès au message original conservé dans une base de données, si bien que la protection de leur sphère privée passe par une absolue transparence des opérations de traçage et de leur finalité, par la mise à disposition d'une fonction de suppression physique des messages privés reçus, ainsi que par un avertissement avant toute suppression définitive d'éléments privés afin de permettre leur sauvegarde.

En matière de *suppression de messages*, le premier risque provient du fait que les messages sont par défaut *supprimés de manière logique*, soit simplement déplacés dans un dossier d'éléments supprimés, où ils restent parfaitement lisibles tant qu'une seconde suppression physique et définitive n'a pas été effectuée (manuellement ou par vidage automatique en quittant). Un utilisateur averti devrait connaître la fonction permettant de supprimer définitivement certains messages! Il subsiste cependant un deuxième risque lié à la procédure de sauvegardes automatiques des données de messagerie, étant donné qu'un *message supprimé peut encore figurer sur des supports de sauvegarde* établis entre le moment de sa réception et celui de sa suppression physique.

En dernier lieu, l'employé peut définir des *délégués disposant d'autorisations d'accès* (lecture, création, modification et/ou destruction) sur certains dossiers de son bureau électronique. Pour ce qui est de la boîte de réception des messages, un délégué peut en cas de besoin envoyer un message ou répondre au nom du titulaire, recevoir ou non une copie des messages relatifs à ses réunions et voir ou non ses éléments privés (nouveaux messages, de même que rendez-vous, contacts et tâches le cas échéant). La meilleure protection des messages privés consiste bien sûr à les conserver dans un *dossier personnel* protégé par un mot de passe et stocké sous forme cryptée sur une unité non partagée mais néanmoins régulièrement sauvegardée.

Pour conclure ce thème, on peut encore relever que la messagerie Internet (boîte aux lettres externes accessibles par le biais des protocoles POP3 ou IMAP4) est en général désactivée par l'employeur pour des raisons évidentes de sécurité. S'agissant des messageries basées entièrement sur le Web, dont certaines supportent le cryptage et la signature numérique des courriels, l'employé peut y trouver un intérêt privé ou professionnel.

2.2.4. Problèmes de sécurité sur les réseaux locaux et personnels sans fil

Comme toute nouvelle technologie, l'essor des réseaux locaux et personnels sans fil (wireless) amène son lot de problèmes liés à la sécurité et la protection des données. L'avantage du «sans fil» en terme d'allégement de l'infrastructure physique câblée et de mobilité des utilisateurs est contrebalancé par un risque accru d'écoute des communications (en principe par fréquences radio). Par conséquent, les normes «sans fil» doivent impérativement inclure un protocole de chiffrement des transmissions, que seule une infrastructure à clés publiques permet vraiment de réaliser, avec toutes les contraintes techniques et organisationnelles que cela implique.

Pour les réseaux locaux (LAN: Local Area Networks), le standard «sans fil» IEEE 802.11 associé au protocole de chiffrement WEP (Wired Equivalent Privacy) vient compléter le standard «câblé» 802.3 (Ethernet) très répandu dans le marché. L'expérience a néanmoins démontré que le WEP n'est pas toujours mis en service et que certaines failles ou difficultés (clés de chiffrement statiques à définir dans chaque équipement) peuvent subsister même lorsqu'il est actif. De plus, les points d'accès sans fil 802.11 partagent la bande passante à disposition (jusqu'à 11 Mbps avec 802.11b et 54 Mbps avec 802.11a) entre tous les équipements mobiles situés dans un périmètre de quelques centaines de mètres, à la différence des commutateurs 802.3 qui individualisent la bande passante (10 ou 100 Mbps) pour chaque équipement fixe câblé et restreignent ainsi incidemment les possibilités d'écoute globale des communications. Pour s'associer avec un point d'accès actif, il est essentiel que l'équipement mobile sans fil connaisse et transmette le nom du point d'accès (SSID: Service Set IDentifier) dans sa requête et surtout qu'il utilise le procédé d'authentification à clés partagées (protocole WEP avec une clé de 104 bits complétée par un vecteur d'initialisation de 24 bits). Une faiblesse de l'algorithme RC4 utilisé par ce protocole réside précisément dans la haute probabilité de réutilisation d'un même vecteur et démontre combien l'implémentation de solutions cryptographiques reste complexe!

Pour les réseaux personnels (PAN: Personal Area Networks) assurant la communication sans fil entre ordinateurs portatifs, assistants numériques personnels, téléphones cellulaires et autres équipements individuels, le standard IEEE 802.15 se base sur la norme Bluetooth qui offre un débit de 732 kbps dans un rayon d'une dizaine de mètres. Elle prévoit fort heureusement une authentification des partenaires et un chiffrement des communications, soit des mesures nécessitant à nouveau une gestion de clés. Les équipements ne comportant aucun clavier de saisie semblent ainsi condamnés à devoir partager une clé définie par défaut, ce qui les exposent à des écoutes voire même à des redirections sauvages. En tous les cas, l'expérience montre qu'il y a lieu de rester vigilant durant la phase de démarrage d'une telle technologie.

Dans un périmètre encore plus local, on assiste à la prolifération des claviers et souris reliés sans fil avec leur poste de travail. Si le côté ergonomique et pratique de cette évolution est incontestable, il faut garder à l'esprit que le clavier sert fréquemment à introduire des mots de passe permettant un accès à des informations sensibles et que ce type de transmission sans fil n'est vraisemblablement pas trop difficile à capter et décoder.

2.2.5. Identification biométrique et les risques inhérents à cette méthode

La biométrie permet d'identifier de manière précise une personne à l'aide de certaines de ses caractéristiques corporelles. De nombreuses parties du corps sont uniques et restent inchangées tout au long de la vie. L'avantage de cette méthode d'identification est l'absence de risques de perte, contrairement aux mots de passe ou de transmission à autrui. De ce fait, l'identification biométrique est estimée comme étant particulièrement sûre. Néanmoins, mis à part les avantages du point de vue de la sécurité et de la protection des données, l'identification biométrique implique également des risques considérables.

Depuis les événements du 11 septembre 2001, l'identification biométrique a le vent en poupe. Ses auteurs la prônent comme étant le moyen le plus efficace de lutte contre le terrorisme puisque les caractéristiques biométriques sont extrêmement difficiles à falsifier. Or cet aspect est de peu de poids si les systèmes d'exploitation ne sont pas sûrs et si des personnes non autorisées peuvent détourner les données biométriques. Des études ont souligné la vulnérabilité de certains systèmes de biométrie proposés dans le commerce. On ne peut donc les mettre en œuvre de manière judicieuse que si les caractéristiques biométriques sont conservées dans un environnement absolument sûr. A cet égard, il est déterminant que le système de vérification ne puisse pas seulement comparer les données avec les modèles enregistrés, mais qu'il puisse aussi contrôler si les données proviennent de la même personne au moment de la vérification. Lorsque le système est incapable de procéder à ces deux contrôles, il y a un risque au niveau de la sécurité. Si les systèmes biométriques présentent aujourd'hui encore des risques, c'est entre autres parce que la biométrie est une technique récente et n'a pas dû surmonter, dans la pratique, de véritables épreuves.

Néanmoins, il est décisif qu'une solution soit trouvée au problème de la sécurité étant donné que l'atout majeur de l'identification biométrique - l'immuabilité des caractéristiques - peut s'avérer en réalité une faiblesse grave. En effet, les données biométriques volées ou perdues ne peuvent plus être remplacées comme un mot de passe ou un certificat. En cas de perte, l'identification biométrique est compromise pour toujours et n'est plus utilisable. C'est la raison pour laquelle l'un des problèmes majeurs des systèmes biométriques aujourd'hui est d'annuler une caractéristique pour que l'on n'en fasse pas un usage abusif. Se tourner vers une caractéristique non compromise n'est qu'une solution apparente car tant que l'identification est effectuée, par exemple, à partir d'un seul doigt, les autres doigts sont encore une solution de rechange. Cela dit, leur nombre est limité.

Les risques actuels que les systèmes d'exploitation biométriques font courir à la sécu-

rité doivent être éliminés pour que les données biométriques puissent être mises en œuvre dans l'optique d'une sécurité élevée et d'une protection efficace des données. En effet, on ne peut remplacer des données biométriques volées.

2.2.6. Exigences fondamentales en matière de protection de la sphère privée dans le domaine des cartes à puce

Les cartes à puce sont désormais très présentes dans la vie quotidienne. Pour que leur utilisation ne mette pas en danger la sphère privée, il suffit de respecter quelques exigences fondamentales.

Bien que les cartes à puce soient remises aux utilisateurs, elles continuent à faire partie du système de traitement de données des services émetteurs. Ceux-ci doivent donc veiller à ce que les mesures techniques et organisationnelles nécessaires soient prises pour, par exemple, empêcher les personnes non autorisées d'y accéder. Cette protection de l'accès est particulièrement importante lorsqu'il s'agit de cartes multifonctionnelles utilisées en commun par plusieurs entreprises. Dans ce genre de cas, il doit être garanti que chacun de ces services n'a accès qu'aux données qui lui sont destinées.

Du fait que la mise en œuvre de cartes à puce implique certains risques pour la sphère privée, leurs détenteurs doivent être informés de manière claire et transparente de leur mode d'utilisation, des risques inhérents à cette utilisation ainsi que de leurs droits. Ils doivent savoir à quel service il convient de s'adresser pour être informés des données saisies et où ils peuvent procéder à la rectification et la suppression de celles-ci. Il doit leur être garanti que les données saisies ne peuvent être lues, transmises à des tiers ou modifiées que si les personnes concernées en sont informées. Celles-ci doivent également être au fait des conséquences d'une perte de la carte et de ce qu'il convient d'entreprendre dans ce cas.

Soulignons également que le service émetteur a le devoir de détruire les données saisies dès qu'il n'en a plus besoin (pour plus de détails sur les cartes à puce dans le domaine de la santé, voir page 59).

2.2.7. Application de la sécurité des données dans l'administration fédérale

L'application des mesures techniques et organisationnelles relatives à la protection des données, respectivement des mesures de protection des données n'avance que très lentement. Bien que le Conseil fédéral ait encore une fois, suite au rapport annuel de l'Unité de stratégie informatique de la Confédération, rendu attentif au fait que les directives de sécurité des données devaient être entièrement respectées au sein de l'administration fédérale, nous constatons régulièrement que ces directives ne sont pas suffisamment respectées. Ainsi, les responsables pour la protection et la sécurité des données ne se voient pas accordé le statut nécessaire au sein des unités d'organisation et en particulier dans les projets informatiques. A notre avis, une solution permettant d'optimiser l'application des directives de protection des données serait de nous donner la possibilité de soumettre nos recommandations qui n'ont pas été suivies ou qui ont été rejetées à la Commission fédérale de la protection des données pour décision.

Seule une infime partie des projets informatiques de l'administration fédérale est annoncée auprès de l'Unité de stratégie informatique de la Confédération (USIC) et nous est remise. L'annonce se fait avec la demande de projet conformément au standard de l'administration fédérale pour la conduite et le déroulement de projets informatiques au sein de l'administration fédérale (HERMES). Cette demande doit déjà contenir des premières indications sur les aspects de protection et de sécurité des données. Environ la moitié des projets annoncés ne fournissent aucune indication à ce sujet. On pourrait résoudre ce problème en exigeant que le mandat de projet ne puisse être adopté que s'il est muni de la signature du délégué à la protection ou à la sécurité des données. Cet instrument de contrôle est cependant rarement utilisé.

D'autre part, la position accordée au responsable de la protection des données au sein d'une organisation permet rapidement de voir si les exigences de la protection des données sont prises au sérieux. Il est bien sûr également nécessaire que ces collaborateurs fassent partie des commissions et participent aux conférences appropriées afin d'être en mesure de déceler très rapidement les écarts entre ce qui est prévu et ce qui est effectivement réalisé. Nous devons constater régulièrement que, dans la majorité des cas, la disponibilité des systèmes est assurée de manière adéquate. La non-disponibilité d'un système est immédiatement constatée par l'ensemble des utilisateurs de même que par la direction, ce qui fait que la pression exercée pour améliorer le système augmente. Dans les domaines, dans lesquels la disponibilité constitue une nécessité absolue, les éventuels coûts résultant d'une panne peuvent être quanti-

fiés de manière assez précise, ce qui permet de voir clairement quel effort doit être fourni pour améliorer le système.

La chose se présente un peu différemment en ce qui concerne les deux autres composants de la sécurité des données. Confidentialité et intégrité sont dans la majorité des cas moins bien quantifiables. Une application insuffisante peut cependant causer des dégâts considérables. Il ne faut pas sous-estimer les atteintes à l'image de marque qui sont occasionnées lorsque des cas de violation de la protection ou de la sécurité des données sont portées à la connaissance du public. Selon des sources proches des médias, seul 3 % environ de ces violations sont connues. C'est la raison pour laquelle il est difficile pour les organes dirigeants de faire appliquer des mesures plus poussées.

Le Conseil fédéral a stipulé dans les normes légales relatives à la protection des données que, lors de traitements de données personnelles sensibles, les exigences de la protection des données devaient être appliquées en utilisant les technologies les plus modernes. Dans un domaine soumis à une évolution aussi rapide que l'informatique, il est cependant difficile de trouver le temps de se préoccuper des problèmes de la protection et de la sécurité des données. Comme il est plutôt difficile de convaincre quelqu'un de la nécessité de ces tâches et qu'elles pourraient sans autre faire surgir certains conflits «créatifs», on se décide malheureusement souvent à éviter ces tâches.

Dans le domaine de l'administration fédérale, nous avons aujourd'hui la possibilité, dans le cas où une disposition de la protection des données ne serait pas respectée, d'émettre une recommandation à l'intention de l'organe responsable. Si cette recommandation n'est pas suivie ou est rejetée, l'affaire peut être soumise au département concerné pour décision. Si le rejet est maintenu, nous ne disposons plus d'autres moyens pour insister sur le fait que les exigences de la protection et de la sécurité des données doivent être appliquées. C'est pourquoi nous sommes d'avis que le régime appliqué dans le domaine du droit privé devrait également être appliqué au sein de l'administration fédérale afin que nous ayons la possibilité de soumettre nos recommandations – qui ont été rejetées ou n'ont pas été suivies par les départements ou par l'administration fédérale – à la Commission fédérale de la protection des données pour décision. Une telle norme permettrait également aux instances dirigeantes de l'administration fédérale de s'appuyer sur des exigences qui permettent un travail conforme aux directives.

2.2.8. Les aspects de la protection des données lors de téléinterventions (Remote Access Tools)

Lorsqu'une intervention à distance est effectuée sur un PC, il faut veiller à ce que seul le propriétaire ou l'organe responsable autorise l'exécution de ces travaux. La communication entre les deux ordinateurs doit être cryptée pour éviter que des tiers puissent intercepter des données interprétables. L'accès aux systèmes doit avoir lieu de manière à ce qu'un accès aux données personnelles (fichiers) ne soit pas possible ou seulement dans des cas isolés, à moins que les données sensibles soient stockées sous forme cryptée. Les travaux de maintenance doivent être journalisés en accord avec les dispositions de la révision et les journaux doivent être régulièrement dépouillés.

Une intervention à distance peut être effectuée par des responsables systèmes ou application propres à l'entreprise ou par des spécialistes d'unités d'organisation externes (entreprises informatiques). Dans les deux cas, il existe un risque que des informations puissent être soustraites de manière incontrôlée. Chaque société devrait connaître la valeur de ses données clients. C'est pourquoi cela étonne d'autant plus que l'on met souvent ces données «à disposition» des experts de la téléintervention sans prendre les mesures de sécurité nécessaires.

Les possibilités de s'attaquer aux systèmes ou aux données dans le cadre de travaux de maintenance sont nombreuses. En principe, la personne ou l'unité d'organisation qui fait l'objet d'une telle intervention, qu'elle soit de nature réparatrice ou préventive, doit donner son accord pour cette intervention, par exemple en lançant un programme sur son PC. Une telle procédure garantit que les téléinterventions ne pourront pas être effectuées de manière incontrôlée.

Il faut d'autre part veiller à ce que les données transmises ne puissent pas être consultées en clair ou copiées par d'autres personnes. Les données doivent impérativement être transmises sous forme cryptée. Un autre point important à respecter lors du traitement de données sensibles est de stocker les données sous forme cryptée afin que celles-ci – au cas où elles seraient accessibles dans le cadre de travaux de maintenance ou d'assistance – ne puissent pas être interprétées. S'il devait être nécessaire pour la correction d'un problème de décrypter les données, ceci doit se faire sous une forme bien contrôlée, par exemple en appliquant le principe des «quatre yeux».

Il va de soi que les mots de passe ou les clés qui sont nécessaires au décryptage des données ne doivent pas être accessibles aux personnes non autorisées. L'accès ne devrait pas être protégé uniquement par des mots de passe, mais dans les domaines sensibles d'une unité d'organisation également au moyen de cartes à puces ou de

systèmes biométriques. L'accès doit être limité aux données qui sont absolument nécessaires pour l'accomplissement de la tâche. Un téléchargement de fichiers dans le cadre de travaux de maintenance ou de réparation doit être impossible, en particulier pour des systèmes sensibles, car ceci empêcherait pratiquement tout contrôle.

Toute intervention sensible, telle qu'une maintenance à distance ou une correction d'erreurs sur des systèmes de production, doit être journalisée sous une forme qui répond aux exigences de la révision. Cela signifie notamment qu'il ne doit pas être possible à posteriori de modifier ou de supprimer des données du journal, du moins pas de manière non contrôlée. Les journaux doivent être conservés pour une année et les ressources doivent être mises à disposition pour effectuer un dépouillement régulier de ces derniers.

Il est conseillé pour les travaux de maintenance à distance de rédiger un contrat écrit qui règle les mesures techniques et organisationnelles qui s'imposent.

2.2.9. L'application de mesures de protection des données pour la statistique suisse des condamnations pénales

Dans les systèmes statistiques, les organes fédéraux doivent veiller à ce que les données personnelles soient anonymisées ou pseudonymisées dès que le but du traitement le permet. La première étape de l'anonymisation pour la statistique des condamnations pénales consiste à créer des identificateurs, la deuxième à créer des numéros d'identification pour la base de données de production. Une anonymisation complète de l'identificateur n'est pas possible avec le système actuel, étant donné que l'identité des personnes peut changer au cours du temps, par ex. par mariage (changement de nom, de lieu d'origine, de nationalité). C'est pourquoi un identificateur pseudonymisé «parlant» a été créé, qui permet de mettre en relation une nouvelle identité avec d'autres identités déjà présentes, pour autant que ces dernières aient déjà été enregistrées dans la base de données des condamnations pénales. L'exemple montre entre autres qu'une anonymisation ou une pseudonymisation des données occasionne dans nombre de cas des frais moindres pour la sécurité des données.

Les données pour la statistique des condamnations pénales proviennent du casier judiciaire informatisé (VOSTRA), d'environ 170 établissements d'application des peines et mesures, de 26 services d'exécution des peines ou de probation ainsi que de 26 offices des tribunaux des mineurs. Ces jugements pénaux sont mis à disposition de l'Office fédéral de la statistique (OFS) par voie électronique une fois par semaine, mais pas sous forme pseudonymisée «parlante». Nous avons rendu attentif l'OFS au fait

qu'il n'est autorisé à se procurer ces données que sous une forme pseudonymisée appropriée. Les admissions et les sorties des établissements pénitentiaires, de même que les jugements concernant des mineurs et les indications relatives aux cas de probation sont communiqués à l'OFS à l'aide de formulaires, sur disquettes ou par voie électronique sous une forme pseudonymisée «parlante». Les données en provenance du casier judiciaire qui ne sont pas pseudonymisées sont cryptées moyennant un algorithme propriétaire avec une longueur de clé de 72 bits. La loi sur la protection des données exige que les traitements de données sensibles soient effectués en utilisant les techniques les plus modernes qui soient disponibles pour les mesures de sécurité. Dans le cas présent, le réseau de données du DFJP ne satisfait – à ce jour – pas encore à ce critère. Les algorithmes symétriques qui sont à la pointe de la technique ne sont pas propriétaires, mais accessibles publiquement et utilisent une longueur de clé de 128 bits au moins. Quelques exemples de telles clés sont: 3DES, IDEA ou AES.

La pseudonymisation «parlante» est effectuée en utilisant des abréviations du contenu des champs suivants qui constituent ensuite l'identificateur: nom, nom d'alias, prénom, sexe, date de naissance, lieu ou pays de naissance, lieu d'origine ou nationalité, domicile et état civil. La pseudonymisation permet de déduire de l'identité d'une personne les données pseudonymisées qui sont stockées dans la base de données des condamnations pénales, pour autant que celles-ci aient déjà été enregistrées. Par contre, l'identification d'une personne sur la base des données d'identification stockées dans la base de données est rarement possible. Pourtant, ce risque existe bel et bien, en particulier lorsque les personnes concernées ont des noms courts. Ce problème doit également être encore mieux résolu.

Le traitement des données pseudonymisées «parlantes» pour le domaine des condamnations pénales est effectué à l'OFS par une équipe de trois personnes environ, ce qui signifie que l'accès aux données est limité. La base de données de production à laquelle un nombre plus élevé de personnes ont accès utilise des numéros d'identification qui sont en relation avec les données personnelles pseudonymisées «parlantes» (identificateur). Ceci signifie qu'une identification des personnes n'est pas possible dans la base de données de production. L'exemple démontre également que les exigences envers la sécurité des données sont moindres lorsqu'on travaille avec des données pseudonymisées. Seule la partie du système qui permet la dépseudonymisation doit encore être considérée comme sensible (niveau de protection 3/niveau de sécurité le plus élevé). Du point de vue de la protection des données, les autres parties du système ne doivent plus être protégées avec des mesures de ce niveau.

2.2.10. Fuite de données au World Economic Forum

Les adversaires de la mondialisation ont profité des faiblesses du système informatique du Forum économique mondial (World Economic Forum WEF) pour entrer en possession de données personnelles concernant certaines personnalités du monde économique et politique. Ces données ont été envoyées à divers médias, qui les ont publiées.

Dans son édition du 4 février 2001 ainsi que dans plusieurs éditions ultérieures, le Sonntagszeitung et d'autres médias par la suite ont publié un certain nombre d'articles sur une action de piratage émanant d'opposants à la mondialisation sur le serveur Internet du Forum économique mondial. Selon ces articles, les pirates seraient parvenus à entrer en possession des noms, numéros de passeport, numéros de téléphone portable et privé, numéros de cartes de crédit, adresses électroniques, noms d'utilisateur et mots de passe de milliers de participants au Forum. En outre, ces informations contenaient semble-t-il des remarques subjectives sur certaines personnalités du monde politique et économique.

Le Sonntagszeitung est entré en possession de ces données à partir d'un CD-ROM. Il nous a fait parvenir des exemples de commentaires et de remarques subjectives sur certains participants au Forum.

Sur la base de ces informations ainsi que du fait que les méthodes de traitement utilisées par le Forum étaient susceptibles de violer la personnalité d'un grand nombre de personnes (erreur de système), nous avons décidé de procéder à un contrôle au siège du Forum. A cette occasion, nous avons tenu tout particulièrement à présenter à la direction du Forum les principes généraux de la protection des données comme le principe de transparence, le principe de proportionnalité et le principe de finalité. Nous avons notamment souligné le fait que la LPD requière du maître d'un fichier que celui-ci protège les données personnelles par des mesures techniques et organisationnelles adéquates contre tout traitement non autorisé. Par ailleurs, nous avons également conseillé à la direction de faire analyser régulièrement les processus informatiques et de faire procéder à des contrôles de sécurité périodiques. La direction a pris connaissance de nos suggestions et les a mises en pratique.

2.3. Autres thèmes

2.3.1. Traitement de données personnelles sur mandat (outsourcing) dans le secteur privé

Aujourd'hui, les traitements de données personnelles demeurent de moins en moins dans la seule compétence du responsable du traitement. Ces traitements sont en effet souvent confiés à des tiers pour des raisons diverses notamment d'ordre économique, technique ou liées aux compétences et moyens à disposition. Ils ne sont pas sans risque pour le respect des droits de la personnalité des personnes dont les données sont sous-traitées. Nous recommandons dans ces cas de conclure un contrat de protection des données.

Le traitement de données sur mandat (outsourcing) recouvre tous les traitements incombant au responsable du traitement, mais effectués par un tiers qui ne lui est pas subordonné. Il peut s'agir de procédés manuels ou informatisés. Ces traitements sur mandat peuvent englober l'ensemble des opérations de traitement ou uniquement certaines phases bien délimitées. Ils sont régis par la loi fédérale sur la protection des données (LPD). Ainsi, si certaines conditions définies par la loi sont respectées, le traitement de données par un tiers est un motif justificatif permettant de traiter et de faire traiter des données personnelles sans porter atteinte à la personnalité des personnes concernées. Le mandant doit cependant garder la maîtrise sur les données dont il confie le traitement à un tiers.

Le mandat doit porter sur des prestations spécifiques limitées à un projet ou une affaire déterminée. Le tiers mandaté est ainsi un «auxiliaire» du mandant. Il n'a pas de compétence de décision par rapport aux données qu'il est appelé à traiter. Il ne peut pas déterminer quelles données doivent être collectées et traitées et ne peut pas les traiter pour ses propres besoins. Dans le cadre du mandat, le mandataire ne doit traiter que les données qui ont été mises à disposition par le responsable du traitement ou qu'il a collectées pour le compte du mandant. Il n'y a pas de rapport contractuel entre le mandataire et la personne concernée. La garantie des droits de la personne concernée relève en principe de la responsabilité du mandant. Le traitement sur mandat au sens de la LPD ne couvre pas le mandat qui entraîne un transfert de fonction et qui confère aux mandataires le traitement des données de manière autonome. Dans ce dernier cas, le mandant n'a plus la maîtrise sur les données. Le tiers mandaté devient le responsable du traitement et jouit d'une grande liberté dans la manière de remplir le contrat en dehors de toute instruction du mandant. Il peut utiliser les données pour ses propres finalités et il est responsable de la licéité des traitements qu'il effectue.

Pour pouvoir évoquer le motif justificatif du «traitement des données personnelles par un tiers», le responsable du traitement doit d'une part veiller à ce que ne soient pas effectués des traitements autres que ceux que lui-même est en droit d'effectuer, c'est-à-dire de veiller à ce que le tiers mandaté se conforme aux impératifs de protection des données dans la même mesure que lui-même y est tenu. Il doit d'autre part vérifier qu'aucune obligation légale ou contractuelle de garder le secret n'interdit la sous-traitance. Le responsable du traitement doit donc veiller au respect des exigences de la protection des données par le tiers mandaté. Il demeure à l'égard de la personne concernée le premier responsable du traitement. Il ne doit pas seulement prendre en considération des éléments de coûts et de rationalisation. Il doit aussi attacher une grande importance au savoir-faire et à la qualité.

Le responsable du traitement doit en particulier s'assurer que la sécurité des données est garantie. Il procédera à une évaluation des risques liés au traitement sur mandat et notamment il s'informera des mesures techniques et organisationnelles prises par le partenaire potentiel et au besoin demandera des compléments. Il doit également définir les prestations attendues, sur le plan quantitatif et qualitatif, soumettre le mandat à un contrôle de prestation strict et prévoir des mesures au cas où les prestations attendues ne seraient pas fournies. Cet aspect de la qualité ne réside pas dans le fait de savoir si le traitement était exécuté plus rapidement avec des outils informatiques plus performants. Il s'agit avant tout et essentiellement de s'assurer que le mandataire respectera les exigences de la protection des données. Celui-ci doit en particulier autoriser le contrôle des activités de traitement, que ce soit par le mandant, le préposé fédéral à la protection des données ou un organe de révision indépendant.

Suivant l'importance du mandat et notamment la sensibilité des données traitées ou le nombre de personnes concernées, le traitement doit être documenté et faire l'objet d'une révision informatique. Il serait d'ailleurs souhaitable qu'une telle obligation de révision soit introduite dans la LPD, non seulement pour le traitement sur mandat, mais pour tout traitement automatisé d'une certaine ampleur ou comportant des données sensibles ou des profils de la personnalité.

Si le responsable du traitement doit transférer des données au tiers mandaté dans le cadre de l'exécution du mandat, cette communication ne constitue pas une communication à un tiers «indépendant» lorsqu'il conserve la maîtrise sur les données transférées. Cela a notamment pour conséquence que le responsable du traitement n'a pas à faire valoir un motif justificatif autre que le mandat pour le transfert des données et qu'il n'a pas à annoncer le fichier si les conditions de l'annonce sont remplies (voir 3e rapport d'activités 1995/96, p. 205). Par contre, il demeure tenu de respecter les conditions de la LPD pour le transfert de données à l'étranger.

La LPD permet l'outsourcing pour le traitement de données personnelles effectué par des personnes privées. Toutefois, ce type de traitement ne doit pas entraîner un affaiblissement de la protection des données. Dans l'intérêt du mandant, nous lui recommandons de conclure un contrat de sous-traitance avec le tiers mandaté, dans lequel seront fixées les règles de protection des données à respecter. En fonction du type de mandat, il conviendrait d'aborder notamment les points suivants:

- le respect des dispositions de protection des données, notamment le règlement des conditions cadres pour le traitement des données (étendue du traitement);
- la finalité du traitement;
- la fixation des mesures techniques et organisationnelles appropriées pour garantir un haut niveau de protection des données et la confidentialité (prise en compte de l'état de la technique, journalisation, contrôle d'accès, chiffrement);
- la séparation du traitement des données - en particulier s'il s'agit de données sensibles ou de profils de la personnalité - des autres traitements opérés par le tiers mandaté afin d'éviter des conflits entre les intérêts du mandant et ceux du mandataire (notamment en relation avec ses propres traitements ou ceux qu'il effectue pour d'autres mandants);
- le cryptage des données sensibles et des profils de la personnalité, si les collaborateurs de l'entreprise mandatée n'ont pas besoin de lire ou de traiter les données dans l'accomplissement de leurs tâches;
- les exigences pour l'engagement du personnel;
- la sous-traitance éventuelle par le tiers mandaté. Il convient en particulier de régler ce qui peut être sous-traité et à quelles conditions. Le mandant devrait en tous les cas être informé par le tiers mandaté des sous-traitants auxquels il fait appel;
- les conditions d'accès éventuel à des données personnelles lorsque le mandataire a accès à distance aux ordinateurs du mandant pour des travaux d'entretien;
- les conditions d'accès aux installations du mandant;
- la soumission du mandataire et de ses employés au respect de la confidentialité;
- le contrôle du respect des dispositions contractuelles, notamment une révision informatique par un organe externe;
- le règlement des responsabilités en cas de dommage ou de non-respect du contrat;
- la peine conventionnelle dont le montant doit être dissuasif pour le mandataire

d'utiliser les données de manière contraire au contrat et aux dispositions de protection des données;

- le devoir d'information du mandataire à l'égard du mandant sur la manière dont se déroule concrètement le traitement;
- la fin du contrat et notamment ce qu'il advient des données une fois le mandat exécuté.

2.3.2. Le registre informatisé de l'état civil

La Confédération a l'intention de créer une banque de données électronique pour la tenue des registres de l'état civil. Conformément à un projet de loi soumis au Parlement, le Conseil fédéral est tenu de veiller à la protection des données. Nous avons à plusieurs reprises exprimé nos doutes à propos de ce projet de loi du point de vue de la protection des données. Nos propositions n'ont néanmoins pas été prises en compte par le DFJP, département compétent en la matière.

La Confédération entend informatiser la tenue des registres de l'état civil. A cet effet, les quelque 1750 offices de l'état civil devront être mis en réseau. Il est donc prévu de créer une banque de données centrale, dénommée Infostar, qui sera exploitée par la Confédération sur mandat des cantons et utilisée par les offices de l'état civil mis en réseau au niveau national. Ce fichier informatique nécessite une base légale dans le code civil. Il est proposé à cet égard de charger le Conseil fédéral de la haute surveillance sur la tenue des registres de l'état civil et de la protection de la personnalité et des droits fondamentaux des personnes dont les données seront traitées dans Infostar. Le fichier ainsi envisagé contiendra l'ensemble des données d'état civil de toutes les personnes domiciliées en Suisse. Ce sera l'un des plus importants fichiers électroniques de données actuelles et sensibles en Suisse. Le projet de révision prévoit aussi qu'Infostar devra remplir en parallèle des fonctions qui dépassent les tâches conférées à l'origine aux offices de l'état civil. Ainsi, les autorités de l'état civil des cantons et de la Confédération ne seront pas les seules à avoir accès à Infostar, mais selon le message, de nombreuses autres autorités pourront aussi utiliser le fichier à leurs propres fins bien que leur mission première ne porte absolument pas sur la tenue des registres de l'état civil.

La LPD ne s'applique pas aux registres publics relatifs aux rapports juridiques de droit privé (art. 2, al. 2, let. d LPD). Les registres de l'état civil, donc Infostar, entrent dans cette catégorie. Il convient de tenir compte de la protection des données directement dans la législation concernée (code civil, ordonnance sur l'état civil). Nous avons donc

demandé que lors de la création des bases légales pour un projet de fichier informatisé comme Infostar qui intervient fortement dans la personnalité de chaque individu, les principes fondamentaux de la LPD soient pris en considération.

Nous avons également souligné à plusieurs reprises que le droit d'accès, élément majeur de la protection des données, et ses modalités, doivent être réglementées expressément dans une base légale formelle. Nous avons soumis une proposition circonstanciée qui réglemente de manière complète le droit d'accès et sa portée, les restrictions, la forme et le contenu de l'octroi de renseignements. Pour des raisons de transparence, nous avons aussi proposé que le code civil mentionne qui gère cette banque de données et quelles autorités traitent les données.

Etant donné que tant les autorités fédérales que cantonales sont habilitées à traiter des données dans Infostar, il faudrait établir expressément dans le code civil qui est compétent en matière de surveillance, cela afin de garantir une répartition claire des compétences entre Confédération et cantons. Infostar est la première banque de données dont la surveillance n'est pas soumise aux mêmes règles que les autres fichiers électroniques de la Confédération. Les banques de données comme le Système de traitement des données relatives à la protection de l'Etat (ISIS) ou le Registre central des étrangers (RCE) sont soumises à la même surveillance, donc uniforme, celle du PFPD. Mais justement du fait qu'un très grand nombre d'autorités (offices de l'état civil, ainsi que d'autres autorités fédérales et cantonales) auront accès à Infostar, il est extrêmement important qu'une surveillance uniforme soit exercée par un organisme indépendant. Nous estimons que le Conseil fédéral en qualité d'autorité de surveillance ne peut exercer cette fonction. La véritable activité de surveillance ne peut être effectuée que par un service compétent et spécialisé comme le PFPD. Cette solution permettrait aussi de garantir que les personnes privées peuvent s'adresser à un service neutre et indépendant lorsqu'elles ont des questions relevant du droit de la protection des données.

Le message relatif à la révision partielle du code civil a été transmis au Parlement par le Conseil fédéral. Les recommandations mentionnées ci-dessus n'ont pas été prises en considération par le DFJP, département compétent en la matière.

2.3.3. La publication d'arrêts du Tribunal fédéral sur Internet

Depuis le 23 avril 2001, le Tribunal fédéral publie presque tous ses jugements dans leur intégralité sur Internet. Ces publications mentionnent les noms des représentants des parties et dans un nombre restreint de cas même ceux des personnes en cause. Le Tribunal fédéral examine chaque cas séparément en pesant les divers intérêts qui sont en jeu.

Depuis le 23 avril 2001, le Tribunal fédéral (TF) publie presque tous ses arrêts dans leur intégralité sur Internet. Ces publications mentionnent les noms des représentants des parties et dans certains cas même ceux des parties en cause. Plusieurs personnes nous ont contactés à ce sujet pour nous demander si cette pratique était admissible en vertu de la loi sur la protection des données. Il y a lieu à ce sujet de retenir tout d'abord que le TF examine chaque cas séparément et pèse les divers intérêts en jeu, notamment ceux des parties concernées. Selon le cas, la publication n'aura pas lieu ou ne sera que partielle. Le TF supprime en règle générale les noms des parties avant la publication. Dans un nombre restreint de cas, où il n'y a pas d'intérêts prépondérants des personnes concernées, les noms des parties sont publiés.

Une publication de jugements requiert une pesée des divers intérêts en jeu. D'une part, le public a un intérêt à prendre connaissance des arrêts du TF, entre autres pour être en mesure d'assurer un certain contrôle (transparence de la justice). Il est également important que le public et les avocats connaissent la jurisprudence. D'autre part, la publication de jugements risque de porter atteinte à la liberté personnelle des parties. Ce problème soulevé par la publication de jugements de tribunaux a également été discuté dans la doctrine. Il est impératif pour la compréhension d'un jugement de disposer d'une description précise des faits relatifs au litige. Il est ainsi parfois inévitable que le lecteur puisse par déduction tirer des conclusions sur des parties qui n'ont pas été nommément citées, par ex. dans les cas où le litige ou les parties impliquées sont bien connues du public. La doctrine a retenu à ce sujet que ce risque devait être accepté au vu du principe de publicité des débats ainsi qu'au fait que la loi sur la protection des données permet la communication des données accessibles au public.

En ce qui concerne la publication des noms des avocats, il ne faut pas oublier que ces derniers sont soumis au secret de fonction et que ceci vaut également pour le cas publié. Un avocat a en outre – selon le TF – une fonction particulière en sa qualité de «serviteur du droit» et de «collaborateur de la justice».

Ceci signifie que la pratique du TF mentionnée ci-dessus, qui consiste à examiner l'opportunité d'une publication d'un jugement pour chaque cas en tenant compte des divers intérêts en jeu, respecte la législation en matière de protection des données.

2.3.4. Systèmes électroniques de contrôle d'accès dans les domaines skiables

Un contrôle des abonnements de ski doit respecter les dispositions de la loi sur la protection des données dès qu'il y a traitement de données personnelles. Dans les cas où une enquête est effectuée sur ordre d'un juge ou confor-

mément à une base légale, il est permis de suivre l'utilisation d'un abonnement de ski et de communiquer les résultats aux organes de police ou à un tribunal. Il n'est pas permis de suivre de manière systématique l'utilisation d'abonnements de collaborateurs, un tel suivi n'est admissible que dans des cas isolés remplissant certaines conditions.

L'organe de coordination de plusieurs chemins de fer de montagne nous a soumis un certain nombre de questions concernant un système électronique de contrôle d'accès qui enregistre tous les abonnements de ski. Nous avons retenu que des traitements de données en rapport avec le suivi d'abonnements de ski (quelle installation a été utilisée quand et avec quel abonnement) ne sont admissibles que s'ils respectent les dispositions de la loi sur la protection des données (LPD). Cela signifie notamment que les principes généraux de la protection des données – licéité, bonne foi, proportionnalité, finalité, exactitude et sécurité des données – doivent être respectés. Conformément à l'art. 13 LPD, un tel traitement nécessite en outre un motif justificatif. Cette règle est applicable indifféremment du fait que l'abonnement a été acheté ou qu'il a été remis à titre gracieux. Lors de suivis anonymes des abonnements, aucune donnée personnelle au sens de la LPD n'est traitée. De tels traçages ne sont donc pas soumis à la LPD. Un traçage d'abonnement n'est cependant considéré comme anonyme que s'il n'est plus possible après coup d'identifier son titulaire.

Il n'est permis de suivre un abonnement de ski et de communiquer les résultats aux organes de police ou à un tribunal que si cette opération est effectuée sur ordre d'un juge ou qu'elle repose sur une base légale. L'organe de coordination des chemins de fer de montagne est autorisé à communiquer les données aux organes de police pour autant que celles-ci soient indispensables pour le dépôt d'une plainte.

Finalement, la question a été soulevée de savoir dans quelle mesure des cartes de collaborateurs pouvaient être surveillées afin de déceler d'éventuels abus. Dans ce cadre, en plus des dispositions de la loi sur la protection des données, les dispositions du droit du travail sont applicables, notamment l'art. 26 de l'ordonnance 3 relative à la loi sur le travail. Une surveillance permanente du comportement des collaborateurs n'est pas autorisée. L'art. 26 al. 1 de l'ordonnance 3 relative à la loi sur le travail n'est cependant pas applicable de manière absolue. Des bases de données ou des systèmes de surveillance tels que des systèmes électroniques de contrôle d'accès peuvent être utilisés *dans des cas isolés* pour surveiller le comportement si toutes les conditions ci-dessous sont remplies:

- Il existe un intérêt prépondérant de l'employeur. Ceci est le cas par exemple lorsqu'il s'agit de déceler des abus.

- La surveillance du respect du règlement d'utilisation relatif au système électronique de contrôle d'accès se fait au moyen de contrôles ponctuels et sans enregistrer le nom et l'adresse, mais par exemple uniquement le numéro d'abonnement.
- Le décodage du numéro d'abonnement pour retrouver le titulaire ne sera effectué que si un soupçon concret d'abus existe.
- Les collaborateurs ont été préalablement informés de ces mesures.

Ces conditions sont applicables indépendamment du fait que les collaborateurs ont reçu leurs abonnements de ski gratuitement ou non. Les conditions mentionnées doivent également être respectées dans le cas où les dépouillements seraient effectués uniquement à des fins internes. Comme nous l'avons mentionné plus haut, le personnel doit être préalablement informé de sorte qu'un consentement n'est alors plus nécessaire.

2.3.5. Formulaires d'inscription pour les appartements à louer

Une régie immobilière a fait preuve d'une réticence certaine quant à l'application du jugement rendu par la Commission fédérale de la protection des données à propos des formulaires d'inscription pour la location d'appartements. Elle estimait qu'un bailleur était en droit de demander, sans avoir de scrupules, de plus amples renseignements à un futur locataire. Nous avons rendu une recommandation contre ce genre de procédé; la régie immobilière l'ayant refusée, nous avons porté le cas devant la Commission fédérale de la protection des données. Le texte de la recommandation ainsi que le recours et l'exposé des motifs sont reproduits page 132.

Suite à la demande qui nous a été adressée par une personne privée, nous avons prié une régie immobilière genevoise de nous faire parvenir l'un de ses formulaires d'inscription destinés à la location d'appartements. Après examen, nous avons constaté que, sur plusieurs points, ce formulaire allait à l'encontre du jugement du 21 novembre 1996 rendu par la Commission fédérale de la protection des données (Jurisprudence des autorités administratives de la Confédération, JAAC, 62.42B) dans le domaine des baux à loyer et ne tenait aucun compte de l'aide-mémoire sur les formulaires d'inscription pour la location d'appartement, rédigé peu après ce jugement par le PFPD. Nous avons informé la régie immobilière de ces observations et exigé une adaptation du formulaire dans le sens du jugement et de l'aide-mémoire susmentionnés.

Malgré l'échange de plusieurs courriers, la régie immobilière ne se montrait toujours pas disposée à adapter ses formulaires d'inscription. Elle défendait le point de vue selon lequel il était indispensable, avant de choisir le futur locataire, de disposer de

renseignements supplémentaires (par exemple l'adresse de l'ancien propriétaire, le loyer payé jusqu'ici, le numéro d'immatriculation du véhicule, si la personne avait fait l'objet de poursuites et quand), et demandait que les personnes intéressées par une location soient tenues de joindre à leur demande les documents suivants: le livret de famille ou la carte d'identité (pour les ressortissants suisses), le permis de séjour (pour les étrangers), une feuille de salaire et un extrait du registre des poursuites. En outre, les locataires potentiels devaient signer une déclaration de consentement autorisant le bailleur, en l'occurrence la régie immobilière, à recueillir auprès de l'employeur et du dernier propriétaire toutes les informations sur la solvabilité, l'emploi, le salaire, les paiements du loyer jusque là effectués, ainsi que sur les poursuites et les actes de défaut de biens. Par ailleurs, elles devaient accepter que ces informations soient également recueillies par une société de renseignements économiques.

La régie immobilière a avancé comme argument le fait que les personnes intéressées par la location d'un appartement apposent leur signature sur le formulaire d'inscription et donnent de leur plein gré les renseignements demandés. Elle méconnaît en l'occurrence la portée du consentement de la victime au sens de l'art. 13 al. 1 LPD. Ce consentement doit se faire en tant qu'acte de libre choix véritable, c'est-à-dire volontairement et en connaissance des conséquences qui en découlent. Les personnes désirant louer un appartement ne peuvent en général pas se permettre de ne répondre qu'à certaines questions figurant sur le formulaire d'inscription car ce faisant, elles s'excluraient elles-mêmes de la liste des candidats potentiels à la location de l'appartement en question. De plus, lorsqu'une personne cherche d'urgence à se loger, on ne peut admettre que le traitement des données en question soit justifié par le consentement de cette personne. Cependant, si un bailleur requiert des données qui ne sont pas nécessaires à la conclusion du contrat, il doit attirer expressément l'attention des locataires potentiels sur le fait que la réponse à ces questions est libre et que l'absence de réponse n'aura pas de répercussions négatives sur leur demande de location.

Dans notre recommandation, nous avons souligné entre autres que le traitement de données opéré par la régie immobilière doit respecter rigoureusement le principe de la proportionnalité. Appliquée au cas ici présenté, cela signifie que l'on ne peut exiger des locataires potentiels et que l'on ne peut ultérieurement traiter que les données qui sont utiles et véritablement nécessaires d'une part au choix du locataire et d'autre part à la conclusion proprement dite du contrat de location. Il n'y aucune raison justifiant que l'on demande une copie du permis de séjour ou de la carte d'identité dès le dépôt du formulaire d'inscription. Uniquement dans l'hypothèse où une disposition légale le prévoit (par ex. en cas d'obligation légale d'annoncer la présence d'une personne), ces documents peuvent être requis lorsque le bailleur ou la régie se sont déci-

dés définitivement pour un locataire. Par ailleurs, on ne peut encore demander d'autres documents que s'ils sont absolument indispensables à la conclusion du contrat ou si une obligation légale l'exige. Dans tous les cas néanmoins, ces documents ne peuvent être demandés à la personne définitivement choisie qu'au moment où la conclusion du contrat est imminente. Les documents qui n'entretiennent pas un rapport direct avec la conclusion du contrat de bail ne peuvent être requis qu'avec le consentement clair et sans équivoque de la personne concernée; à cet effet, il convient de mentionner sans ambiguïté qu'il est facultatif de joindre ces documents au formulaire d'inscription.

La régie immobilière a rejeté notre recommandation dans le sens des considérations présentées ci-dessus. Nous avons porté l'affaire devant la Commission fédérale de la protection des données pour décision.

3. Justice/Police/Sécurité

3.1. Affaires de police

3.1.1. Expériences avec le droit d'accès indirect

Le nombre des demandes de renseignement indirectes dans le domaine de la police est en augmentation durant la période 2001/2002. Le traitement des demandes relatives à la sûreté intérieure et à la lutte contre le blanchiment d'argent s'effectue sans problème. Par contre, celui des demandes relatives au crime organisé, au trafic illicite de stupéfiants, à la fausse monnaie, à la traite des êtres humains et à la pornographie pose quelques problèmes liés à la nature même du système JANUS.

Le nombre des demandes de renseignement indirectes déposées 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) a augmenté de manière significative durant la période 2001/2002. Ce phénomène est en grande partie dû aux traitements de données personnelles effectuées 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 (voir également à ce sujet texte G8 p. 50). Quant au nombre des demandes de renseignement indirectes fondées sur la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC), il a également augmenté mais dans une moindre mesure.

Le traitement des demandes relatives au système ISIS s'effectue toujours sans problème. C'est également le cas pour les demandes fondées sur la LOC concernant le système GEWA de l'Autorité de contrôle en matière de lutte contre le blanchiment d'argent.

En ce qui concerne le système JANUS, la situation décrite dans notre 8ème rapport d'activités 2000/2001 (p. 137 et 138) n'a pas fondamentalement changé et nous avons adressé une nouvelle fois une recommandation à l'OFP lui demandant de garantir que lors de l'examen des demandes toutes les données personnelles de la personne requérante qui sont traitées par la Police judiciaire fédérale (PJF, anciennement les Offices centraux de police criminelle de la Confédération) puissent être vérifiées conformément à la LOC. Cette recommandation a été dans un premier temps rejetée par l'OFP, alors même qu'il avait accepté la recommandation mentionnée dans notre 8ème rapport d'activités qui traitait du même problème. Avant de porter l'affaire devant le DFJP et dans le but de débloquer cette situation, une séance réunissant le Préposé fédéral et la direction de l'OFP s'est tenue à la fin du mois de décembre 2001. Suite à cette réunion, l'OFP s'est engagé à remédier aux problèmes soulevés dans nos recommandations.

3.1.2. Contrôles de sécurité relatifs aux personnes au sein de l'administration fédérale

La nouvelle ordonnance sur les contrôles de sécurité relatifs aux personnes touche un nombre important de collaborateurs. Les traitements de données effectués doivent d'autant plus être conformes au principe de proportionnalité. Cette nouvelle ordonnance devra prochainement être complétée notamment par une liste des données personnelles qui seront traitées dans le système électronique de gestion des contrôles de sécurité.

Le Conseil fédéral a donné au DDPS le mandat de réviser l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP). Le DDPS a constitué un groupe de travail interdépartemental qui a élaboré un projet de révision totale de l'OCSP dont les points principaux sont une nouvelle procédure de contrôle de sécurité comportant trois degrés, une répétition des contrôles et une nouvelle définition des offices et des fonctions à risques.

En matière de protection des données, deux points ont retenu notre attention. Premièrement, le nombre de personnes soumises à un contrôle de sécurité étant très important, nous avons rappelé que tout traitement de données personnelles devait respecter le principe de proportionnalité. Deuxièmement, l'OCSP prévoit, sur la base de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

(LMSI), la mise en place d'un système électronique relatif aux contrôles de sécurité. Celui-ci ne constitue pas un système d'information nécessitant une base juridique spécifique. Le DDPS devra cependant procéder assez rapidement à des modifications de l'OCSP, notamment introduire la liste des données personnelles qui seront traitées dans le système mentionné ci-dessus.

L'OCSP est entrée en vigueur le 1er janvier 2002. Nous poursuivrons nos tâches d'accompagnement et de conseil en particulier lors de l'introduction dans l'OCSP de la liste des données personnelles traitées dans le système de gestion des contrôles de sécurité.

3.1.3. Révision de l'art. 179quinquies CP pour «la protection des mouvements d'affaires»

L'enregistrement des conversations téléphoniques sans le consentement des personnes concernées ne doit avoir lieu que dans les cas d'appels de détresse dans le sens où ces appels sont adressés à un numéro d'urgence comme par exemple le 117 ou le 118. Dans le contexte des mouvements d'affaires, un tel enregistrement à l'insu des personnes concernées constitue une atteinte injustifiable à la vie privée.

L'art. 179quinquies CP stipule que dans le cas où la personne concernée n'aurait pas été informée au préalable, seul l'enregistrement des appels de détresses pour le compte de services d'assistance, de secours ou de sécurité n'est pas punissable. Tous les autres enregistrements de conversations téléphoniques sans le consentement de l'ensemble des interlocuteurs sont punissables sur plainte. Donnant suite à une initiative parlementaire visant la révision de l'art. 179quinquies CP pour «la protection des mouvements d'affaires», le Conseil des Etats a chargé sa Commission des affaires juridiques d'élaborer un projet d'acte législatif. Avec la collaboration du Département fédéral de justice et police, ladite Commission a proposé d'étendre l'exception de l'art. 179quinquies CP à l'enregistrement de toutes les conversations téléphoniques avec des services d'assistance, de secours ou de sécurité et à l'enregistrement de conversations téléphoniques auxquelles participe un entrepreneur pour autant que l'enregistrement en question soit uniquement utilisé à titre de preuve concernant le contenu commercial de la conversation.

La notion d'«appel de détresse» figurant dans l'actuelle disposition pénale pose aux services d'assistance, de secours ou de sécurité le problème de l'arrêt de l'enregistrement ou de l'information des personnes concernées sur le fait que la conversation est enregistrée lorsqu'il apparaît que le contenu de celle-ci ne constitue pas un appel de détresse. Tout en reconnaissant cette situation problématique, nous esti-

mons que la solution proposée, à savoir l'enregistrement de toutes les conversations téléphoniques avec des services d'assistance, de secours ou de sécurité, va bien au-delà du problème à régler. En effet, le projet de révision permet l'enregistrement d'appels téléphoniques pour l'ensemble des organes des services d'assistance, de secours ou de sécurité (numéros d'appel d'unités administratives, de renseignement ou numéros internes de collaborateurs de ces services) et cela indépendamment qu'il s'agisse d'appels de détresse ou non. Du point de vue du principe de proportionnalité, la possibilité légale d'enregistrement à l'insu de l'interlocuteur ne doit pas porter sur des appels tels que ceux cités ci-dessus. L'enregistrement sans le consentement de la personne concernée ne doit avoir lieu que dans les cas d'appels de détresse dans le sens où ces appels sont adressés à un numéro d'urgence comme par exemple le 117 ou le 118.

Le projet de la Commission des affaires juridiques du Conseil des Etats prévoit également la possibilité d'effectuer un enregistrement d'une conversation téléphonique sans aucune information des personnes impliquées lorsque l'une d'elles est un entrepreneur. Le projet précise que l'utilisation des enregistrements est destinée notamment à des fins de preuves concernant le contenu commercial de l'entretien ou la levée d'éventuels malentendus. Une atteinte à la vie privée tel que l'enregistrement d'une conversation téléphonique à l'insu de l'interlocuteur n'est pas justifiée dans le contexte des mouvements d'affaires, de tractations et de conclusions de contrats. L'enregistrement avec le consentement de tous les interlocuteurs permet sans aucun problème la conservation de preuves et la levée d'éventuels malentendus dans un tel contexte. Il faut aussi noter que les acteurs économiques, désirant soigner leur image de marque, ont un intérêt à respecter les conditions minimales favorisant la transparence. Le projet de révision de l'art. 179^{quinquies} CP est actuellement traité par le Parlement.

3.1.4. Révision des ordonnances dans le domaine de la police

La réforme des structures policières (StruPol) du Département fédéral de justice et police a impliqué l'élaboration de nouvelles ordonnances et la modification d'ordonnances déjà existantes. Nous avons examiné dans le cadre de la consultation des offices tous ces textes légaux et avons constaté qu'ils répondaient de manière générale aux exigences de la protection des données.

Comme nous l'avons déjà mentionné dans notre 8ème rapport d'activités 2000/2001 (p. 133 à 135), des remaniements ont eu lieu au sein de l'Office fédéral de la police (OFP), suite au projet de réforme des structures policières (StruPol) du Département fédéral

de justice et police (DFJP). Ces restructurations ont impliqué des modifications de textes légaux, notamment en ce qui concerne les dispositions de protection des données. Nous avons examiné dans ce cadre plusieurs ordonnances du Conseil fédéral qui répondent dans l'ensemble aux exigences de la protection des données. Nous n'avons pas eu de remarques à formuler ou toutes les divergences ont été aplanies dans la majorité des cas.

Dans trois cas, les divergences ont été mentionnées dans la proposition au Conseil fédéral qui a tranché en faveur de l'office concerné. Il s'agit en premier de l'ordonnance sur les mesures visant au maintien de la sûreté intérieure. Nous avons soutenu que les informations provenant de l'étranger qui ne remplissent pas les conditions fixées par la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (informations inutiles ou inexactes) doivent être détruites ou retournées à l'expéditeur et non simplement classées sans autre forme de traitement. Le deuxième cas a trait à l'ordonnance sur le traitement des données signalétiques où nous avons demandé de remplacer l'effacement sur demande de la personne concernée par l'effacement d'office en cas d'acquittement. Le troisième cas concerne l'ordonnance sur le système informatisé de la police judiciaire fédérale (ordonnance JANUS) qui prévoit une durée de conservation des données de huit années que nous avons jugée disproportionnée.

Finalement, dans le cadre de la procédure de consultation des offices relative à la nouvelle ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police qui remplace l'ordonnance sur les Offices centraux de police criminelle près l'Office fédéral de la police, nous avons fait remarquer que les tâches de la Police judiciaire fédérale (PJF) devraient être réglées, à l'instar des anciens Offices centraux de police criminelle de la Confédération, dans une loi au sens formel. L'OFP s'est engagé à élaborer une telle loi prochainement.

3.1.5. Communication de données policières dans le cadre du sommet du G8 à Gênes

Le Parti Socialiste Suisse nous a demandé d'examiner les conditions dans lesquelles les autorités suisses ont communiqué aux autorités italiennes des données policières dans le cadre du sommet du G8 à Gênes. Nous avons procédé à une analyse juridique de la situation et effectué deux contrôles auprès de l'Office fédéral de la police. Nous sommes parvenus à la conclusion que la communication de données personnelles aux autorités italiennes dans le cadre du sommet du G8 s'est déroulée conformément à la loi.

Par lettre du 18 juillet 2001, le Parti Socialiste Suisse nous a interpellés au sujet de la communication par l'Office fédéral de la police (OFP) de données personnelles aux autorités de police italiennes en marge du sommet du G8 à Gênes. Le Parti Socialiste souhaitait en particulier savoir selon quels critères était défini la notion d'opposant violent à la globalisation, la provenance des données transmises aux autorités italiennes, les bases légales d'une telle communication et les garanties de protection des données entourant ce traitement.

Nous avons examiné cette requête en procédant en premier lieu à une analyse juridique détaillée de la situation. Nous avons ensuite effectué deux contrôles directement auprès de l'OFP. Nous avons également saisi l'autorité de protection des données italienne afin qu'elle contrôle dans le cadre de ses compétences le traitement par les autorités de police italiennes des données personnelles provenant de l'OFP. Cette requête est encore pendante.

Il est ressorti de notre analyse juridique que la responsabilité de l'enregistrement des données dans le système de traitement des données relatives à la protection de l'Etat (système ISIS) revient au Service d'analyse et de prévention (SAP) de l'OFP. Il doit le faire en conformité avec les dispositions de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) et de l'ordonnance ISIS. Il doit en particulier définir les critères exacts qui justifient l'enregistrement au sens de la LMSI. Les traitements de données font l'objet de contrôles à plusieurs niveaux: le service de contrôle interne du SAP, le Département fédéral de justice et police, la Délégation des Commissions de gestion et le Préposé fédéral à la protection des données. Nous avons en outre relevé qu'une personne qui participe à une manifestation de manière non violente et sans commettre d'acte répréhensible, ne doit pas être enregistrée dans le système ISIS. En ce qui concerne la communication des données, notre analyse montre que les données communiquées proviennent d'ISIS et leur communication ne peut intervenir que conformément à l'article 17, alinéas 3 à 5, resp. 7 LMSI. Le SAP est responsable de la licéité de la communication à des autorités étrangères. Toute communication de données, y compris ses destinataires, son objet et ses motifs doivent être enregistrés dans ISIS. Sur la base de cet enregistrement, il est possible d'examiner le respect des dispositions légales. Le destinataire des données ne peut les utiliser que pour les finalités pour lesquelles les données lui ont été transmises. Il est informé des limites mises à l'utilisation et le SAP peut exiger des informations sur la manière dont les données ont été utilisées. Un contrôle auprès du pays destinataire n'est possible que par les autorités de protection des données dudit Etat, dans la mesure où de telles autorités existent, ce qui est le cas de l'Italie.

Suite à cette analyse juridique nous avons procédé les 24 juillet et 9 août 2001 à deux contrôles dans les locaux du SAP. Lors de ces contrôles nous avons vérifié si les auto-

rités italiennes avaient effectivement demandé des informations au SAP, quelles autorités italiennes étaient impliquées, quel a été le rôle de l'agent de liaison envoyé à Gênes par le SAP dans la communication des données, quelles données ont été transmises (nombre de personnes ou d'organisations concernées, personnes suisses ou étrangères etc.), les bases légales de la communication, le respect des conditions de la LMSI et de l'ordonnance ISIS et l'enregistrement des communications dans ISIS. Nous avons également vérifié si le SAP avait reçu des données personnelles des autorités italiennes.

Le SAP a mis à notre disposition l'ensemble des documents (pièces de dossiers et extraits d'ISIS) concernant la communication de données personnelles aux autorités italiennes. Il a également mis à disposition les documents entrants (informations communiquées au SAP ou demandes qui lui ont été adressées).

Sur la base des informations exhaustives que nous a fournies le SAP et des constatations que nous avons faites, nous sommes parvenus à la conclusion que la transmission de données personnelles aux autorités italiennes lors du sommet du G8 à Gênes s'est déroulée dans le cadre légal fixé par les articles 3 et 17 LMSI, ainsi que l'article 13 de l'ordonnance ISIS. La communication était indispensable à la sauvegarde d'intérêts importants liés à la sûreté de la Suisse ou de l'Etat destinataire (art. 17, 3e al., let. d LMSI). En outre conformément à l'article 13, 4e et 5e al. ordonnance ISIS, les destinataires ont été informés sur la fiabilité et l'actualité des données. Ils ont été rendus attentifs au fait que les données ne doivent être utilisées que dans le but pour lequel elles leur ont été transmises. La communication, ainsi que ses destinataires, son objet et ses motifs ont été enregistrés de manière conforme dans le système ISIS. Les données ont été communiquées par l'intermédiaire d'un agent de liaison sur place ou au moyen d'un fax crypté.

Lors d'une audition le 21 août 2001, nous avons également informé en détail la Délégation des Commissions de gestion du Parlement des démarches que nous avions entreprises dans le cadre de cette affaire et des résultats de nos investigations.

3.1.6. Les Accords de Schengen sous l'angle de la protection des données

Suite à l'importance politique prise au cours de l'année 2001 par les mandats de négociation d'adhésion de la Suisse aux Accords de Schengen, nous avons été amenés à examiner ces derniers sous l'angle de la protection des données. Notre analyse a montré que du point de vue des standards légaux de protection des données à mettre en place, la Suisse répond de manière adéquate aux conditions demandées. Par contre, afin de pouvoir adhérer

aux Accords de Schengen, un certain nombre de problèmes devront au préalable être examinés et plusieurs adaptations législatives devront être entreprises.

L'analyse que nous avons effectuée nous a amenés à rappeler qu'une adhésion de notre pays aux Accords de Schengen aurait des conséquences du point de vue de la protection des données. Nous avons ainsi relevé que les problèmes liés à une telle adhésion ne doivent pas être vus dans l'optique d'un affaiblissement de la protection des données du fait de la participation à un système international de coopération. Au contraire, du point de vue de la protection des données, l'avantage d'une telle adhésion est qu'elle placerait les traitements de données nécessaires aux échanges d'informations avec les parties contractantes dans un cadre bien défini et délimité, qui répond à des exigences élevées conformes au standard du droit européen en matière de protection des données. Cette adhésion permettrait un meilleur encadrement des flux d'informations et donc de meilleures garanties pour les personnes concernées, grâce notamment à une stricte limitation des finalités et des utilisations possibles des données.

Dans le cadre de notre analyse, nous avons mis en évidence trois conséquences à prendre en compte sous l'angle de la protection des données en cas d'adhésion de la Suisse aux Accords de Schengen:

Premièrement, nous avons relevé que la Suisse répond, d'une manière générale et au niveau fédéral, aux standards légaux à mettre en place et aux exigences fixées dans les Accords de Schengen. La Suisse dispose de normes législatives suffisantes en matière de protection des données. Peuvent principalement être mentionnés l'article 13 de la Constitution qui consacre le droit de tout individu à la protection de la sphère privée, la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, la Recommandation n° R (87) 15 sur l'utilisation des données à caractère personnel dans le secteur de la police, la loi fédérale sur la protection des données et son ordonnance d'application, les lois fédérales formelles spécifiques qui régissent les systèmes informatisés de police qui pourraient être concernés par les Accords de Schengen et les dispositions de protection des données y relatives.

Deuxièmement, nous avons établi une liste de problèmes qui devront être réglés avant de pouvoir adhérer aux Accords de Schengen. Il conviendra en effet d'examiner la question délicate des cantons, qui d'une manière ou d'une autre, seront également touchés par une adhésion aux Accords de Schengen. Si la majorité des cantons ont aujourd'hui une loi cantonale en matière de protection des données, ils n'ont pas tous institué une autorité de contrôle indépendante et leur effectivité est très différente

compte tenu des structures et des moyens à disposition. Le niveau de protection peut différer entre cantons ou entre la Confédération et les cantons. D'autre part, eu égard aux dispositions des Accords de Schengen régissant le traitement des données personnelles, il conviendra de procéder à un examen détaillé de la situation des différentes banques de données suisses de police et de déterminer quels systèmes d'informations seront concernés (RIPOL, IPAS, AUPER, RCE, ISIS, JANUS etc.). Il conviendra également de régler précisément les flux d'informations et les interconnexions entre les systèmes existants et le Système d'Information Schengen (SIS) national, respectivement le SIS commun ayant fonction de support technique. Il faudra enfin veiller à ce que des dispositions de protection des données identiques s'appliquent au traitement des données en vertu des Accords de Schengen, cela indépendamment du fait que les données proviennent de fichiers fédéraux ou de fichiers cantonaux ou que le traitement soit le fait d'organes fédéraux ou d'organes cantonaux.

Troisièmement, notre analyse a mis en évidence la nécessité d'entreprendre un certain nombre d'adaptations législatives, en particulier pour régler la création d'un SIS national suisse (élaboration d'une base légale formelle), les liens entre le SIS national suisse et les autres banques de données qui l'alimenteront (RIPOL, IPAS, AUPER, RCE, ISIS, JANUS etc.), la participation à une ou des banques de données internationales, les échanges transfrontières de données de police, les mécanismes de contrôle de l'exactitude et de la qualité des données, l'exercice des droits des personnes concernées et notamment le droit d'accès (délimitation entre droit d'accès direct et droit d'accès indirect) ou encore les échanges d'informations liées à la procédure complémentaire dénommée SIRENE (Supplementary Information Request at the National Entry). Ces modifications législatives devront également prendre en compte les problèmes liés aux compétences cantonales de police (notamment collaboration policière entre la Confédération et les cantons, l'accès au SIS etc.), aux compétences des organes de contrôle de protection des données (Préposé fédéral et autorités cantonales de protection des données) ainsi qu'à la participation du Préposé fédéral à l'autorité de contrôle commune.

Notre analyse nous a amenés à conclure que du point de vue des standards légaux de protection des données à mettre en place, la Suisse répond de manière adéquate aux conditions demandées. Par contre, afin de pouvoir adhérer aux Accords de Schengen, les problèmes susmentionnés devront au préalable être examinés et les adaptations législatives nécessaires devront être entreprises.

Les résultats et conclusions de notre analyse ont notamment été transmis au groupe de coordination PESEUS (Groupe de Projet-DFJP-Stratégie-UE-Suisse) du Département fédéral de justice et police. Nous avons également communiqué notre position dans le

cadre des procédures de consultation relatives à des interventions parlementaires sur ces Accords de Schengen de même que lors de notre audition en août 2001 par la Commission de politique extérieure du Conseil des Etats.

3.1.7. Blanchiment d'argent et obligation pour La Poste de copier une pièce d'identité

La Poste demande aux titulaires de comptes jaunes une pièce d'identité officielle dont elle fait une photocopie qu'elle conserve. A ce sujet, nous avons rédigé la feuille d'information «La Poste et la loi sur le blanchiment d'argent» que vous trouverez à la page 126. Cette feuille explique pourquoi la Poste, en vertu de la loi sur le blanchiment d'argent, ne doit non seulement vérifier les pièces d'identité, mais également enregistrer leur contenu essentiel et le conserver.

3.2. Autres thèmes

3.2.1. La révision de la loi sur l'asile

La révision de la loi sur l'asile prévoit la possibilité d'ordonner des analyses génétiques dans le but de faire la lumière sur une situation familiale. Nous sommes d'avis que ceci est disproportionné. Nous avons rendu attentif au fait qu'il fallait, le cas échéant, au moins régler certains points en rapport avec ces analyses génétiques.

Dans le cadre de la révision de la loi sur l'asile, nous avons été invités à prendre position. Nous nous sommes surtout concentrés sur l'introduction d'analyses génétiques. Lors de procédures de regroupement familial, il importe entre autres de faire la lumière sur la vraie situation familiale. Ainsi il est prévu que la loi sur l'asile permettra, après sa révision, d'ordonner des analyses génétiques. Nous sommes d'avis que ceci est disproportionné. Il y a lieu dans ce contexte de tenir compte du fait qu'une analyse génétique constitue pour la personne concernée une atteinte extrêmement grave à sa personnalité. Ni le texte de la loi, ni les explications de cette dernière ne permettent de démontrer la nécessité de prendre une telle mesure. Il faut également relever que la personne concernée n'a aucune possibilité de s'opposer à ce qu'une analyse génétique soit effectuée. Une telle opposition aurait en règle générale pour conséquence – selon le texte de la loi – l'irrecevabilité de la demande d'asile. C'est la raison pour laquelle nous rejetons avec fermeté l'introduction d'analyses génétiques dans la loi sur l'asile.

Nous avons en outre mentionné les points qui devraient être pris en compte dans la révision de la loi au cas où cette disposition permettant d'ordonner des analyses génétiques devrait néanmoins être maintenue. Il faudrait tout d'abord fournir une liste exhaustive des analyses génétiques qui sont autorisées. En fonction de l'analyse génétique, il faudrait ensuite régler certaines modalités dans la loi (par exemple s'il s'agit d'une analyse même ou simplement de l'établissement d'un profil ADN). La loi devrait par exemple prévoir que le résultat ne pourra pas être utilisé à d'autres fins et qu'il soit immédiatement détruit une fois la situation familiale éclaircie.

Les explications de la loi font référence à l'avant-projet de loi fédérale sur l'analyse génétique humaine. Nous sommes d'avis que ceci n'est pas approprié car, contrairement à la loi sur l'asile, l'avant-projet susmentionné présume que la personne concernée donne librement son consentement. Dans le cas de la loi sur l'asile par contre, on ne peut pas parler d'un consentement libre puisque la demande d'asile sera déclarée irrecevable si la personne concernée s'oppose à l'analyse.

3.2.2. Vidéosurveillance dans la gare principale de Zurich

En automne 2001, nous avons procédé à un contrôle des installations de vidéosurveillance des CFF dans la gare principale de Zurich. La surveillance n'est pas transparente pour les passants. Les quelques 100 caméras en partie bien visibles laissent présumer qu'une surveillance est effectuée, une information plus claire à l'aide de panneaux indicateurs fait cependant entièrement défaut.

La vidéosurveillance connaît actuellement un véritable essor. A première vue, elle semble être une recette miracle pour garantir la sécurité des personnes ainsi que pour prévenir les déprédations matérielles; elle dissuade les délinquants et facilite en cas de besoin l'organisation des secours. Nous sommes cependant d'avis qu'il n'est pas avéré qu'une vidéosurveillance renforcée augmente automatiquement la sécurité.

Les principes généraux de la protection des données stipulent qu'une vidéosurveillance ne peut être utilisée que si elle est nécessaire et apte à atteindre les objectifs fixés. Si ce but peut également être réalisé par une atteinte moins radicale à la personnalité des personnes concernées, la vidéosurveillance est illicite. Des mesures techniques et organisationnelles appropriées doivent être prises pour éviter un traitement non autorisé des données de vidéosurveillance. De telles mesures de surveillance doivent donc être soigneusement évaluées.

Si nous avons choisi d'effectuer notre contrôle dans la gare principale de Zurich, c'est que celle-ci est fortement fréquentée par le public et qu'il y existe un nombre élevé

d'installations de vidéosurveillance. Le contrôle a porté uniquement sur les installations de vidéosurveillance des Chemins de fer fédéraux (CFF) ainsi que sur la communication à des tiers de données personnelles enregistrées au moyen de ces installations.

Nous allons par la suite mentionner l'installation de vidéosurveillance «Nœud Zurich» ainsi que celle du centre d'information et de vente des CFF qui sont tous les deux situées dans des espaces accessibles au public.

En plus des quelques caméras installées dans des gares environnantes et qui sont également connectées à l'installation «Nœud Zurich», la gare principale de Zurich compte à elle seule plus de 80 caméras (gare souterraine, passages, accès à l'aile nord et accès central pour livraisons) exploitées sous la responsabilité de la division Infrastructure des CFF. L'installation a été aménagée par la police cantonale de Zurich, qui a elle-même accès à une partie des caméras et peut ainsi être considérée comme co-exploitante de l'installation. Les CFF ne procèdent à aucun enregistrement de données sur cette installation. Il n'existe pas non plus de lien avec un fichier. La transparence de la vidéosurveillance est mauvaise pour les personnes concernées, des panneaux indicateurs ou autres informations font défaut. Les caméras sont en partie peu visibles et ne peuvent être détectées que si l'on regarde de plus près. Les personnes concernées ne savent pas à quoi sert l'installation, qui a accès aux images, si un enregistrement est effectué et si l'installation est reliée avec un fichier.

Une autre installation de vidéosurveillance est installée dans le centre d'information et de vente des CFF, elle surveille les guichets de vente des billets ainsi que l'agence de voyages à l'aide de 16 caméras couleur installées de manière fixe. Les images prises par l'ensemble des caméras sont enregistrées sur cassette vidéo à l'aide d'un système spécial. Le local qui héberge ce système d'enregistrement est fermé à clé. Il n'y a pas de personnel travaillant dans ce local. Un visionnement en temps réel dans le local de contrôle est techniquement possible, mais n'est en règle générale pas effectué. Lorsqu'un incident survient, on avertit la police. Un collaborateur de la police cantonale qui a accès au local de contrôle vient alors prendre la cassette vidéo actuelle pour procéder ensuite à un dépouillement des images. La responsabilité de cette installation incombe à la division Voyageurs des CFF. Les caméras sont plus visibles que celles qui sont installées dans le «Nœud Zurich», mais il n'existe également aucun panneau indicateur. Cela signifie que les personnes concernées ne sont pas informées, en particulier du fait que des images sont prises.

Aucune des installations de vidéosurveillance exploitées par les CFF ne repose d'ailleurs sur une base légale explicite. Seule une base générale existe dans la loi sur les chemins de fer ainsi que dans la loi sur les CFF. Une base légale plus concrète est en préparation.

Nous n'avons pas pu déterminer de manière définitive dans quelle mesure les installations de vidéosurveillance atteignent l'objectif recherché et si ce dernier ne peut pas être également atteint moyennant d'autres mesures qui portent moins atteinte à la personnalité des personnes concernées. Il est nécessaire d'analyser soigneusement pour chaque secteur à risque quelles sont les mesures à prendre pour permettre de minimiser les risques, ceci surtout pour évaluer l'opportunité et la proportionnalité. A l'échéance rédactionnelle, le rapport final de contrôle n'a pas été rédigé étant donné que les faits n'ont pas encore pu être établis de manière définitive. Nous attendons encore les réponses aux questions complémentaires que nous avons posées.

4. Informatique et télécommunication

4.1. Encaissement des redevances de réception radio et télévision

Cette année, l'encaissement des redevances de réception des programmes de radio et de télévision a une nouvelle fois soulevé des questions relatives à la protection des données. A part quelques demandes mineures, celles-ci ont concerné l'accès facilité pour l'organe d'encaissement Billag aux données d'adresse des communes et les traitements de données relatifs à l'exonération de la redevance radio et télévision pour les bénéficiaires de prestations complémentaires AVS/AI.

L'organe d'encaissement Billag, mandaté par la Confédération, nous a informé qu'il rencontrait des problèmes à se procurer les données d'adresses et nous a demandé de rechercher une solution pour contacter facilement les personnes soumises au paiement de la redevance. Billag désire en particulier avoir un meilleur accès aux registres des habitants des communes.

Les fichiers des autorités cantonales ou communales sont soumis aux dispositions de protection des données spécifiques de ces autorités et ne sont donc pas sous notre contrôle. Conformément aux bases légales fédérales actuellement en vigueur, les autorités cantonales ou communales communiquent, sur demande, à l'Office fédéral de la communication (OFCOM) ou à l'organe d'encaissement le nom et l'adresse d'une personne enregistrée pour permettre des contrôles ponctuels de l'obligation de déclarer la réception. Une communication des adresses effectuée de manière régulière (par exemple des nouveaux arrivants dans une commune) n'est pas prévue par l'actuelle législation sur la radio et la télévision.

Nous appuyons tout effort qui permettrait à Billag de faciliter l'encaissement des redevances pour fournir notamment à la SRG SSR idée suisse les moyens financiers dont elle a besoin pour exécuter son mandat légal. Une solution, qui consistera vraisembla-

blement en une adaptation des dispositions légales, devra néanmoins respecter les principes généraux de protection des données, notamment celui de la proportionnalité. Nous avons été invités à discuter ce problème avec l'OFCOM, Billag, Swisscom et la SSR; cet entretien a eu lieu en mars 2002.

Le Tribunal fédéral a décidé en janvier 2001 que toute personne touchant des prestations complémentaires à la rente AVS ou AI – indépendamment du montant des prestations complémentaires ou d'autres conditions – était exonérée du paiement de la redevance. L'ordonnance sur la radio et la télévision a été modifiée en conséquence au 1er août 2001. Sur demande écrite, les personnes qui touchent des prestations selon la loi fédérale sur les prestations complémentaires à l'AVS ou AI sont exonérées du paiement de la redevance. La personne requérante doit fournir à l'organe d'encaissement une décision ayant force de chose jugée concernant son droit aux prestations complémentaires. Du point de vue de la protection des données, cette disposition est à saluer puisqu'elle ne nécessite pas la communication à l'organe d'encaissement de données complémentaires, telles que des informations sur la situation financière, voire sur la santé du requérant. Plusieurs réactions que nous avons reçues indiquent cependant que tout ne semble pas encore être clair. Des personnes concernées nous ont informé qu'elles ont été invitées (par ex. par leur commune) à envoyer à l'organe d'encaissement la décision complète d'attribution de prestations complémentaires. Il serait souhaitable qu'un formulaire uniforme soit créé pour l'ensemble de la Suisse, à l'aide duquel les autorités communales ou cantonales pourraient simplement confirmer que la personne concernée touche des prestations complémentaires de la Confédération et a donc droit à l'exonération de la redevance.

5. Santé

5.1. Thèmes divers

5.1.1. Conditions minimales de protection des données lors de l'établissement d'une carte de santé

Lors d'une conférence de concertation organisée par le Département fédéral de l'intérieur, différents scénarios ont été examinés en vue de l'introduction d'une carte de santé en Suisse. Quel que soit le modèle qui sera finalement retenu, l'introduction et l'acceptation d'une telle carte dépendront en grande partie de la manière dont les exigences de la protection des données seront réalisées. Nous avons précisé à cette occasion les grandes lignes qui devront être prises en considération.

La conférence organisée par le DFI le 30 août 2001 sur le thème de la carte de santé avait pour objectif de trouver un consensus sur le but, le système et le contenu de la carte et sur le rôle que la Confédération était appelée à jouer. Différents scénarios ont été examinés (voir http://www.hospvd.ch/public/ise/carte_sante/) et la Confédération devra assumer un rôle de coordination en collaboration avec l'ensemble des partenaires intéressés. Il s'agira en particulier de favoriser une simplification de la gestion des données des assurés. Dans un premier temps, la carte de santé devrait au moins faciliter la gestion des données administratives des assurés et permettre la réalisation d'économie. Il est ainsi recommandé d'introduire d'abord une carte d'identification des assurés. Elle servirait d'accès aux données de base des assurés (nom, prénom, assureur-maladie, type d'assurance). Cette carte devrait être facultative. A long terme, un système global de transfert et d'accès aux données médicales pourrait être mis en place. Il nécessite au préalable des études et des recherches notamment afin de déterminer les avantages et les inconvénients d'un tel système pour les personnes concernées.

Nous sommes d'avis qu'une carte de santé ne peut pas être introduite à n'importe quelles conditions. En particulier, il est indispensable que les exigences de la protection des données soient d'emblée prises en compte et que le droit fondamental de tout individu à l'autodétermination en matière d'information soit pleinement respecté. Face aux scénarios qui ont été présentés à la conférence de concertation, nous avons émis un avis réservé, car il n'est pas certain que la carte de santé apportera nécessairement une amélioration du respect des droits de la personnalité des patients lors du traitement de données personnelles les concernant et notamment dans les flux d'informations entre prestataires de services (médecins, hôpitaux etc.) et assureurs. Une attention particulière devra être prêtée au contenu de la carte et aux finalités de son utilisation. L'introduction d'une carte de santé doit dès lors se faire dans le respect notamment des conditions suivantes:

- Avoir une assise démocratique. Cela signifie la mise en place des bases légales nécessaires dans une loi au sens formel.
- Respecter la maîtrise des individus sur les données personnelles qui les concernent. Cela postule le caractère facultatif de la carte et la non-discrimination des patients-assurés qui ne recourent pas à la carte. Ceux-ci doivent pouvoir également choisir le type de carte qu'ils souhaitent (carte d'assuré et/ou carte d'accès aux données médicales).
- Délimiter les données figurant sur la carte. La carte doit être conçue comme une carte d'identification du patient, respectivement de l'assuré et éventuellement comme une carte d'accès à d'autres banques de données. Elle ne devrait pas con-

tenir des données médicales, mais uniquement des données d'identification de la personne concernée et des données administratives.

- Garantir la transparence du traitement des données personnelles. Les personnes concernées doivent notamment être pleinement informées des données enregistrées sur la carte, de l'utilisation des données, des finalités poursuivies et des personnes ayant accès à des informations. Elles doivent également connaître les caractéristiques techniques de la carte.
- Garantir l'accès des personnes concernées à leurs données. Les personnes concernées doivent à tout moment pouvoir avoir accès au contenu de la carte ou aux données enregistrées dans des banques de données liées à l'utilisation de la carte, ainsi qu'aux traitements qui en résultent. Ils doivent pouvoir obtenir la rectification ou l'effacement des données fausses.
- Définir clairement les accès aux données si la carte doit être utilisée en tant que carte d'accès à des banques de données. Les accès devront ainsi être réglementés afin que les différents acteurs aient accès aux seules données nécessaires à l'accomplissement de leurs tâches et que le secret médical demeure garanti.
- Assurer la sécurité des données, non seulement lors de la communication des données, mais également lors de leur mémorisation.
- Configurer la carte de santé et traiter les données personnelles qui en résulte en s'appuyant sur les technologies de la vie privée et en recourant aux techniques de pseudonymisation notamment lors de flux de données entre prestataires de services et assureurs.

Nous marquons ainsi une préférence pour un scénario qui garantit le caractère facultatif de l'utilisation de la carte. La Confédération devrait avoir la possibilité de fixer le standard technique de la carte, ainsi que les exigences de protection des données et d'accès sélectif aux données.

5.1.2. La conservation de données médicales dans le secteur privé

Les lois cantonales sur la santé prévoient en règle générale pour les professions médicales un délai de conservation des dossiers médicaux. Au cas ou il n'existe ni disposition professionnelle particulière, ni disposition légale explicite, le délai de conservation doit être conforme au principe de la proportionnalité, c.-à-d. que les documents doivent être conservés aussi longtemps que cela semble nécessaire et opportun. Pour le secteur privé, on peut, en s'appuyant sur le délai de prescription stipulé dans le Code des obligations,

partir du principe qu'un délai de conservation de dix ans est raisonnable à des fins de preuve.

Nous avons été à plusieurs reprises appelés à répondre à la question de la durée de conservation des dossiers médicaux. Cette question est d'importance, autant pour les personnes qui gèrent ces dossiers que pour les patients eux-mêmes, étant donné que ces documents contiennent des informations concernant la santé, données réputées sensibles en vertu de la loi fédérale sur la protection des données (LPD).

Les personnes exerçant une profession médicale trouveront en règle générale des délais précis de conservation dans les lois et ordonnances cantonales sur la santé. Dans de nombreux cantons, le délai de conservation dans le secteur privé (clinique privée ou cabinet médical) est de dix ans. Dans le secteur public (hôpital cantonal), ce délai est souvent plus long et peut être de 20 ans ou plus.

Les personnes exerçant des professions pour lesquelles aucune disposition spécifique n'a été prévue concernant le délai de conservation des dossiers, doivent se conformer aux dispositions générales. De telles dispositions relatives à la conservation de documents tels que les livres comptables existent par exemple dans le Code des obligations. Celui-ci prévoit également un délai de dix ans. Dans le cas des traitements – y compris la conservation – de données personnelles, la plupart des lois renvoient directement à la LPD; cette dernière ne prévoit cependant pas de délais de conservation explicites. Le délai de conservation approprié doit donc être déterminé séparément pour chaque cas en respectant le principe de la proportionnalité (art. 4 LPD). D'une part, les données personnelles ne doivent pas être détruites trop tôt, d'autre part, elles ne peuvent pas non plus être conservées pour une durée indéterminée. L'obligation de conserver les dossiers médicaux est justifiée entre autres par la nécessité de sauvegarder des preuves. Aussi longtemps qu'une affaire n'est pas prescrite, il est possible par exemple qu'on ait besoin de documents comme moyens de preuve dans un procès en responsabilité civile. Dans ce domaine, le délai de prescription commun est de dix ans (art. 127 CO). On peut donc présumer qu'un délai de conservation de dix ans est convenable. Une fois ce délai écoulé, on peut admettre que les données ne sont plus utiles et qu'elles peuvent être détruites ou, si nécessaire, anonymisées.

Dans des cas exceptionnels, il peut être nécessaire de conserver des dossiers médicaux au-delà du délai de conservation prescrit. Ceci peut être le cas par exemple en psychiatrie où le dossier médical précédent peut jouer un rôle important pour le traitement actuel, même si entre-temps le patient n'a pas été en traitement pendant plusieurs années. Même si une telle conservation au-delà du délai de prescription peut très bien être dans l'intérêt de la personne concernée, cela ne signifie pas qu'elle soit

admissible sans autre. Elle nécessite au minimum le consentement tacite de la personne concernée.

Finalement, nous tenons à mentionner encore une fois que le patient peut demander à tout moment – à ses propres risques – qu'on lui remette son dossier ou qu'on le détruise, étant donné que ce dossier contient des données le concernant personnellement et que c'est avant tout dans son intérêt qu'il est conservé. Si le délai de conservation légal n'est pas encore écoulé au moment d'une telle remise ou destruction du dossier, la personne concernée doit – pour autant qu'elle demande qu'on lui remette les originaux et qu'elle interdise l'établissement de copies à des fins de preuve – déclarer sous forme écrite qu'elle libère les personnes tenues par la loi de conserver le dossier de cette obligation et qu'elle renonce à toute revendication découlant de la relation établie dans le cadre du traitement (cf. 8e Rapport d'activité 2000/2001, pages 168 ss).

5.1.3. Adressage insuffisant de courriers confidentiels

L'expéditeur doit veiller à ce que le contenu d'un envoi demeure confidentiel. Lorsque du courrier est adressé par la poste à une institution, l'adresse doit être suffisamment précise pour que l'envoi puisse être remis à la personne concernée sans avoir été préalablement ouvert. Pour garantir ceci, le nom de la personne concernée doit figurer dans l'adresse. Une adresse non personnalisée peut entraîner l'ouverture de l'envoi confidentiel par une personne non autorisée qui aurait ainsi illicitement connaissance du contenu.

Une personne nous a demandé si un envoi à contenu confidentiel adressé à une institution devait comporter dans l'adresse le nom du médecin concerné ainsi qu'une mention spéciale telle que «personnel» ou «confidentiel». Il s'agissait dans le cas concret d'un résultat d'examen qu'un laboratoire avait envoyé à un hôpital sans mentionner le nom du médecin compétent dans l'adresse. Etant adressé à l'hôpital en général, l'enveloppe fut traitée comme l'ensemble du courrier normal, ce qui signifie que le résultat d'examen aboutit à découvert dans la poste interne.

Nous nous étions déjà exprimés précédemment à ce sujet en relevant que l'expéditeur doit veiller à ce que le contenu d'un envoi demeure confidentiel. Cela signifie que l'adresse ne doit contenir ni trop, ni pas assez d'informations (cf. 4e Rapport d'activités 1996/97, pages 223 ss). Si l'expéditeur ne dispose pas des éléments nécessaires à un adressage correct, il doit se renseigner auprès du destinataire. Ceci vaut en particulier dans le cas d'un courrier confidentiel comme l'envoi d'un résultat d'analyse par un laboratoire médical. Nous conseillons en outre d'apposer une mention «confidentiel» ou «personnel» sur de tels envois.

L'adressage à titre personnel ou confidentiel est une mesure simple mais efficace qui assure que les envois confidentiels aboutissent directement chez les bons destinataires. Les personnes concernées, en l'occurrence les patients, ont un intérêt découlant de la protection des données à ce que le nombre de personnes qui prennent connaissance de leurs données médicales demeure aussi restreint que possible. Ceci vaut particulièrement pour les grandes institutions telles que les compagnies d'assurance, les hôpitaux et les administrations. La pratique largement répandue qui consiste à renoncer à adresser les envois à titre personnel n'est pas admissible du point de vue de la protection des données pour les envois à contenu confidentiel, étant donné qu'elle augmente les risques de violation du secret médical. Le fait que les personnes qui prennent connaissance du contenu soient elles-mêmes liées à un secret de fonction est, dans ce cas, sans pertinence.

5.1.4. Le tarif médical Tarmed

Selon les projets de conventions concernant le tarif médical Tarmed, il faudrait indiquer les codes exacts du diagnostic sur toutes les factures des médecins. Il s'agit à ce propos des codes CIM-10 et des codes compatibles ICPC. La transmission systématique à l'assurance-maladie du diagnostic détaillé n'est toutefois pas compatible avec la loi sur la protection des données. Nous recherchons actuellement avec les différents partenaires tarifaires des solutions conformes aux principes de la protection des données.

Les conventions élaborées dans le cadre du tarif médical Tarmed prévoient d'obliger le fournisseur de prestations à transmettre aux assurances des factures médicales contenant les codes exacts de diagnostic. Cela concerne d'une part les assurances-maladie et de l'autre les assurances militaire, invalidité et accidents. Outre les codes CIM-10, les factures des médecins devraient également comporter des donnés de diagnostic selon l'ICPC (International Classification of Primary Care) qui est comparable au CIM. Nous nous opposons depuis des années déjà à la transmission de codes de diagnostic aux assureurs (violation du principe de proportionnalité). Le système de codage CIM-10 a été mis au point à des fins globales de statistique et de recherche et n'est pas approprié au contrôle des coûts et au contrôle du caractère économique des prestations (cf. également 8e Rapport d'activités 2000/2001, p. 167). Le fait est que le projet Tarmed ne répond pas aux exigences de la loi sur la protection des données. Avec ce système, les assurances-maladie recevraient des informations complètes sur les assurés. En raison de l'étroite imbrication entre les différentes assurances (maladie, accident, complémentaire et vie, entre autres), il y aurait, pour les personnes assurées, atteinte aux droits de la personnalité et des patients.

La facturation électronique est un autre point de controverse généré par le nouveau tarif Tarmed. Le fournisseur de prestations risque de transmettre directement les factures aux assureurs sans que le patient en ait connaissance. Le système dit du tiers garant dans lequel le patient est le débiteur et peut décider lui-même s'il veut payer la facture serait de ce fait supprimé (cf. également 8e Rapport d'activités 2000/2001, p. 165). Par ailleurs, la sécurité des données lors de la transmission sera probablement une source de problèmes supplémentaires.

Au cours de l'année écoulée, nous avons invité tous les partenaires de ce système tarifaire à nous informer de l'état d'avancement du projet, à nous fournir des preuves concrètes des besoins en matière de données et à nous soumettre des propositions de solution. En même temps, des pourparlers sont en cours avec divers spécialistes afin d'acquérir une meilleure vue d'ensemble.

Nous estimons nécessaire de s'orienter vers des solutions qui garantissent les droits de la personnalité des assurés et empêchent la «transparence» du patient. Une solution serait de transmettre aux assureurs non pas des données à caractère personnel sur les patients, mais des données pseudonymisées. Les assureurs pourraient tout aussi bien contrôler l'exactitude des factures, ainsi que la qualité des prestations et leur caractère économique.

Enfin, mentionnons l'interpellation Sommaruga (01.3594) du 5 octobre 2001 qui s'exprime de manière critique sur le projet de codes de diagnostic. Dans sa réponse, le Conseil fédéral se prononce clairement contre la transmission systématique de diagnostics détaillés aux assureurs.

5.1.5. Publication sur Internet des valeurs du point appliquées par les dentistes

La rédaction de l'émission «Kassensturz» de la télévision alémanique a publié en août 2001 sur Internet une liste des valeurs du point tarifaire, valeurs qu'elle avait obtenues au moyen d'une enquête par téléphone effectuée de manière cachée auprès d'un millier de cabinets dentaires sélectionnés au hasard. Nous sommes d'avis que la collecte et la publication des données fut dans ce cas contraire aux principes de la loi fédérale sur la protection des données (LPD). Nous avons ainsi demandé le retrait de la liste publiée sur Internet.

Dans le cadre d'une enquête cachée, la rédaction de l'émission «Kassensturz» a collecté les valeurs du point tarifaire d'un millier de dentistes choisis au hasard. Ces valeurs ont été publiées sous forme de liste sur le site Web de «Kassensturz». La liste

mentionne le nom, le numéro postal, la localité, le canton et la valeur du point ou, le cas échéant, la mention «pas obtenu de réponse». Nous sommes d'avis que la manière dont les données ont été collectées est contraire au principe de la bonne foi, étant donné que les dentistes contactés n'ont obtenu aucune information ou des informations fausses sur l'identité de l'appelant ainsi que sur le but de l'enquête. Selon le droit actuel, un dentiste n'est pas tenu de divulguer la valeur du point qu'il pratique. Ces valeurs sont néanmoins accessibles dans la mesure où les dentistes, en règle générale, les communiquent sur demande. Cela ne signifie cependant pas pour autant qu'elles puissent être publiées sans autre dans les médias de masse et en particulier sans le consentement des personnes concernées.

La rédaction de «Kassensturz» justifia sa démarche en invoquant l'intérêt prépondérant du public à connaître ces valeurs. Nous doutons que l'intérêt public soit prépondérant dans le cas présent. D'autre part, même si cet intérêt devait être considéré comme prépondérant, cela ne dispense pas de respecter les principes de la loi fédérale sur la protection des données lors du traitement des données. Un de ces principes est celui de la proportionnalité. Il doit toujours être respecté, même s'il existe un motif justifiant le traitement des données; dans le cas présent donc indépendamment du fait qu'un intérêt prépondérant justifie ou non l'enquête cachée et la publication des données. A notre avis, la publication des valeurs du point sous la forme choisie est contraire à ce principe. Le principe de la proportionnalité exige entre autres que l'on choisisse toujours le moyen qui entrave le moins les droits de la personne concernée. Le fait que le législateur n'ait soumis que certains domaines de prestations à une obligation de communiquer les prix, permet aux autres domaines, dont font partie les dentistes, de conclure à un droit à la non-divulgation. Si ce droit est enfreint pour des intérêts d'ordre public, ceci doit être fait de manière aussi modérée que possible. Le besoin du public à être informé sur les valeurs du point pratiquées par les dentistes aurait pu être satisfait en publiant les résultats de l'enquête de manière anonyme, c.-à-d. sans indiquer les noms. Il n'était pas nécessaire de citer les noms pour atteindre l'objectif souhaité.

Le Département fédéral de l'économie a entre-temps décidé d'élaborer un projet de révision de l'ordonnance sur l'indication des prix visant à faire tomber les prestations des dentistes sous le coup de ladite ordonnance. La publication des valeurs du point appliquées par les dentistes reposera ainsi sur une base légale conforme aux exigences de la loi sur la protection des données.

5.1.6. L'utilisation de données médicales pour des projets intercliniques d'assurance de la qualité

Nous avons analysé un projet dans le domaine de la chirurgie qui a pour objectif de permettre aux cliniques participantes de mesurer aussi bien la qualité de leurs propres prestations que de la comparer au niveau de qualité d'autres cliniques. Nous avons décrit les conditions requises pour une collecte et un traitement de données médicales dans notre 8e rapport d'activités 2000/2001 aux pages 161 ss. L'exemple évoqué ici éclaire surtout les questions relatives à l'organisation, à l'exactitude des données et à la manière de traiter les pseudonymes.

Le but du projet est de mettre en place une méthode qui permette de mesurer la qualité dans les cliniques chirurgicales et d'effectuer une analyse comparative (benchmarking) pour des secteurs d'activité comparables. La méthode peut être découpée en quatre phases distinctes:

- Phase de collecte: les données sont saisies au moyen d'un formulaire dans les cliniques qui participent au projet, puis transmises à un organe central par courrier postal ou par voie électronique.
- Phase de correction: les données sont soumises à un contrôle d'exactitude et, si nécessaire, retournées à la clinique pour correction.
- Phase de saisie: les données vérifiées sont enregistrées dans une base de données centrale.
- Phase de contrôle de la qualité: les données traitées sont gravées sur un CD-ROM qui est mis à disposition des cliniques une fois par année.

Chaque phase de même que chaque passage d'une phase à une autre doit satisfaire à des exigences spécifiques du point de vue de la protection des données.

- Phase de collecte: les patients doivent être informés sur le but de la collecte des données ainsi que sur la communication de celles-ci. Les données saisies sur le formulaire ne doivent pas permettre d'induire directement à l'identité de la personne, ce qui signifie qu'elles doivent être pseudonymisées. Ni le nom, la date de naissance, le domicile ou la nationalité ne doivent apparaître sur le formulaire. Le pseudonyme choisi, un numéro de patient, ne doit être connu qu'au sein de l'établissement médical.
- Phase de collecte à phase de correction: le formulaire doit être envoyé par courrier postal recommandé à l'organe central de dépouillement. La transmission par voie électronique doit être effectuée de manière cryptée (par ex. en utilisant PGP avec une clé de 1024 bits au moins).

- Phase de correction: si le formulaire doit être retourné à la clinique pour effectuer des corrections, l'envoi se fera également comme décrit ci-dessus. D'autre part, l'envoi doit être effectué en respectant le principe des «quatre yeux», ce qui permet pratiquement d'exclure le risque d'un adressage erroné.
- Phase de correction à phase de saisie: les formulaires transmis à l'organe central de dépouillement pour être enregistrés dans la base de données statistiques centrale seront traités par des collaborateurs qui n'habitent pas la région dans laquelle se trouve la clinique dont proviennent les données devant être saisies.
- Phase de saisie: les données des diverses cliniques doivent être enregistrées dans des bases de données séparées afin d'éviter un mélange involontaire des données.
- Phase de contrôle de la qualité: le CD-ROM mis à disposition des cliniques chaque année ne doit contenir que les données de la clinique même ainsi que les données anonymisées des autres cliniques. Tous les pseudonymes doivent être supprimés des enregistrements et aucun attribut permettant de conclure à l'identité d'une personne ou d'une autre clinique ne doit être utilisé.

Le projet montre combien il est important de bien séparer les instances impliquées au niveau organisationnel. La pseudonymisation doit être effectuée au bon moment et la table des correspondances qui permet de retrouver la personne correspondant à un pseudonyme donné doit être protégée contre tout accès par des tiers (cf. 8e rapport d'activités 2000/2001, pages 161 ss).

L'envoi de données personnelles sensibles par courrier postal ou par voie électronique doit se faire avec un soin minutieux (crypté, recommandé, principe des «quatre yeux»). Il faut éviter que des personnes impliquées puissent, grâce à une combinaison fortuite d'attributs, reconnaître une personne.

5.2. Génétique

5.2.1. Exigences minimales de la protection des données dans le domaine des analyses génétiques

Le décryptage du génome humain pose un nouveau défi au législateur. Il s'agit en particulier de garantir le droit à l'autodétermination individuelle en matière d'information et d'éviter toute discrimination en raison du patrimoine génétique. Nous reproduisons ci-dessous quelques principes de protec-

tion des données qu'il convient de respecter dans le contexte des analyses génétiques.

Les processus en matière d'analyses génétiques doivent faire l'objet de dispositions légales. La Suisse possède déjà une base légale dans le domaine des poursuites pénales par exemple. Un projet de loi existe à propos des analyses génétiques dans le domaine de la médecine, de l'emploi, des assurances et de la responsabilité civile. Il devrait être examiné par le parlement dans un proche avenir.

Les analyses génétiques ne doivent en principe être effectuées que sur une base volontaire. Il convient d'éviter toute influence, notamment toute pression individuelle et sociale. Les analyses ne sont autorisées que si la personne concernée y a consenti. Le consentement libre et révocable en tout temps est valable en droit si la personne concernée a été renseignée de manière complète sur cette analyse génétique. Elle doit en particulier être informée du but de l'analyse et des risques qui y sont liés.

Les analyses génétiques doivent être effectuées en fonction du but qui leur a été assigné. Les différents buts doivent être établis dans une loi. Il convient à ce propos de choisir la méthode qui implique extrêmement peu ou pas de données superflues. Ces dernières doivent être immédiatement détruites.

La personne concernée dispose également du droit de ne rien savoir et peut refuser de prendre connaissance des résultats des analyses. Le droit de ne pas savoir revêt une certaine importance parce que bon nombre de maladies ou de risques de maladies peuvent certes faire l'objet d'un diagnostic, mais pas d'un traitement.

Les mineurs et les personnes incapables de discernement tout particulièrement doivent être protégés des analyses génétiques. Par exemple les analyses génétiques chez les personnes incapables de discernement ne peuvent être effectuées que si elles sont absolument indispensables à la protection de leur santé. Cela peut aussi être le cas lorsqu'une maladie grave dans la famille ne peut être établie autrement. Dans tous les cas, il convient de recueillir auparavant, dans la mesure du possible, l'opinion de la personne incapable de discernement.

Dans le domaine du diagnostic prénatal, on ne peut collecter des informations que si elles concernent une lésion curable ou si elles permettent de conclure à une malformation grave de l'enfant. Les examens de dépistage chez les nouveau-nés ne peuvent s'étendre qu'aux dispositions héréditaires curables.

Dans le secteur de l'emploi et des assurances, il convient d'interdire le traitement des données génétiques car c'est en effet un domaine où l'on ne peut exclure les discriminations. Les exceptions ne doivent être autorisées qu'en cas de nécessité absolue.

Il convient enfin d'introduire des normes de qualité à même de garantir une utilisation sûre des données génétiques et, étant donné la sensibilité du sujet, de créer également des normes pénales.

Les principes ici énumérés ne sont pas exhaustifs et les conséquences du point de vue de la protection des données que le décryptage du génome humain impliquera nécessitent que nous poursuivions nos réflexions.

5.2.2. Les problèmes que posent les analyses génétiques dans la pratique

Un cas tiré de la pratique souligne les problèmes que des analyses génétiques ont fait naître du point de vue du droit de la protection des données. Les personnes concernées ne savaient notamment pas dans quel but les données génétiques les concernant allaient être utilisées.

Il s'agissait en l'occurrence d'une famille dont un médecin voulait analyser le patrimoine héréditaire. Les membres de la famille donnèrent leur consentement à ces recherches surtout parce que le médecin leur avait promis un accompagnement médical. Le médecin s'était alors rendu à leur domicile et avait fait une prise de sang à chacun des membres de cette famille. En outre, ces derniers avaient tous été photographiés. Aucune information n'avait suivi, qu'il s'agisse du but des prises de sang, des données génétiques ou des photographies. Il n'y avait eu aucun suivi médical, malgré des demandes réitérées.

Cette famille se sentait atteinte dans ses droits de la personnalité. Elle demanda au médecin d'interrompre immédiatement les travaux de recherche et interdit toute utilisation et transmission de données la concernant. Par ailleurs, les membres de cette famille demandèrent au médecin un rapport circonstancié sur le déroulement des analyses afin de pouvoir déterminer la suite de leur action.

Ce cas montre à l'évidence que le conseil génétique surtout présente encore des lacunes, notamment dans le domaine de la formation des médecins.

Même si la loi fédérale sur la génétique humaine n'est pas encore entrée en vigueur, d'autres dispositions sont aujourd'hui applicables. Outre la loi sur la protection des données et le code pénal, nous mentionnons en particulier les directives médico-éthiques sur la génétique humaine, élaborées et publiées par l'Académie suisse des sciences médicales. Elles décrivent les conditions-cadre, identiques en de nombreux points au projet de loi nommé ci-dessus, sous lesquelles les médecins sont habilités à agir. Ces directives prévoient en particulier que les analyses génétiques doivent être accompagnées d'un suivi génétique complet. Ce suivi et l'accompagnement médical qui va de pair doivent avoir lieu durant et après l'analyse génétique. Le droit de ne rien

savoir et le consentement en tout temps révocable de la personne concernée occupent également une place majeure dans ces directives.

6. Assurances

6.1. Assurances sociales

6.1.1. Lacunes en matière de réglementation dans le domaine de la protection de données médicales

Le Conseil fédéral et nous-mêmes avons été invités dans un postulat (Postulat 99.093 Commission des affaires juridiques du Conseil national) à rédiger un rapport sur les lacunes en matière de réglementation dans le domaine de la protection des données médicales pour l'ensemble du secteur des assurances sociales. L'Institut du droit de la santé de l'Université de Neuchâtel a été chargé de prendre en main cette tâche conséquente.

Dans son postulat du 27 mars 2000, la Commission des affaires juridiques du Conseil national a invité le Conseil fédéral et nous-mêmes à élaborer un rapport sur la protection des données médicales dans l'ensemble du domaine des assurances sociales. Il s'agit en particulier d'examiner l'évolution technologique du traitement électronique des données. La réflexion doit également porter sur la protection pénale du secret en vertu de l'article 321 CP. Le rapport doit permettre de déterminer à temps et de créer les bases et normes nécessaires dans le domaine de la protection des données médicales. L'Institut du droit de la santé de l'Université de Neuchâtel, qui possède une grande expérience en la matière, a été mandaté pour rédiger ce rapport.

De notre point de vue, il s'agit avant tout de savoir si les procédures actuelles dans le domaine des assurances sociales sont conformes à la loi sur la protection des données ou s'il faut éventuellement adapter les dispositions actuellement en vigueur (cf. également 7e Rapport d'activités 1999/2000, p. 167). Il convient également d'examiner l'évolution future dans le domaine des assurances sociales et de souligner les possibilités et les risques d'abus (E-health, informatisation des dossiers de patients, carte de santé etc.). Par ailleurs, il s'agit de présenter les risques dans le domaine de la sécurité des données, de montrer les possibilités techniques et de contribuer à réduire les risques (technologies prenant en compte la protection des données, utilisation des pseudonymes, techniques de cryptage, signatures digitales etc.).

A notre avis, il est par ailleurs essentiel de renforcer le droit à l'autodétermination des assurés en matière d'information. On pensera à cet effet par exemple aux mesures qui

permettent aux patients un accès sûr et aisé à leurs données médicales. Les patients décident qui peut accéder aux données les concernant, quand et comment. Le rapport devrait être terminé à la fin de l'année 2002 et être rendu public ultérieurement.

6.1.2. La CNA et le ficher des «prestataires particuliers»

La CNA tient un fichier permettant de relever les prestataires présentant des caractères particuliers. Nous sommes actuellement en train d'examiner ce fichier sous l'angle de sa conformité avec la législation sur la protection des données.

La CNA possède un fichier dont le but est de permettre un contrôle plus précis des factures émanant de «prestataires ou auteurs de factures particuliers». Il s'agit d'un fichier automatisé, qui nous a certes été annoncé, mais dont nous n'avons pas encore examiné la conformité avec la législation sur la protection des données. Une personne figurant dans ce fichier nous a demandés de procéder à l'examen mentionné ci-dessus.

Nous avons pour mission de contrôler le respect de la loi sur la protection des données (LPD) et des autres prescriptions fédérales en matière de protection des données par les organes de la Confédération. La CNA est à considérer comme un organe fédéral au sens de la LPD. Nous établissons les faits d'office ou sur demande de tiers. A cet effet, nous sommes habilités à requérir des dossiers, à recueillir des renseignements et à demander que l'on nous montre la manière dont les données sont traitées. Les organes fédéraux doivent participer à l'établissement des faits.

Le fichier dont il est ici question est intitulé «Application MediData: contrôle intégral des prestataires». Les utilisateurs «MediData» font partie des catégories de destinataires.

D'une part, on ne sait pas sur quelles bases légales repose le fichier. D'autre part, les notions de «prestataires particuliers» et d'«utilisateurs MediData» ne sont pas claires et nous ne saisissons pas le but précis de ce fichier. La question se pose à ce propos de savoir si l'enregistrement des «prestataires particuliers» est nécessaire et utile (principe de proportionnalité). Nous ne savons également pas quelles données sont traitées dans le fichier et quelle est leur durée de conservation.

6.1.3. Aide-mémoire relatif au thème «Rapport de sortie et d'opération»

Les rapports de sortie et d'opération posent souvent des problèmes dans la pratique. La plupart des assureurs requièrent des hôpitaux des rapports de sortie et d'opération complets, afin de pouvoir établir une appréciation de leur devoir de prestation. Cette pratique n'est toutefois pas compatible avec le principe de la proportionnalité. L'Association suisse des commissaires à la protection des données a publié pour cette raison un aide-mémoire sur ce thème (cf. annexe p. 123).

6.1.4. Traités internationaux dans le domaine de la sécurité sociale et clause de protection des données

Des traités internationaux sont régulièrement conclus entre la Suisse et d'autres Etats dans le domaine de la sécurité sociale. La conclusion de ce genre de traités implique un échange de données relatives aux assurances sociales. Cette transmission doit être réglementée dans une clause spéciale dite de protection des données, tout particulièrement lorsque des données personnelles sont transmises de Suisse vers des pays ne possédant pas une protection des données équivalente. Une clause-type de protection des données se trouve en annexe, page 125.

6.2. Assurances privées

6.2.1. Assurances complémentaires et questions sur l'état de santé

Il est courant, dans la pratique, que les assurances-maladie offrent des assurances complémentaires parallèlement à l'assurance-maladie obligatoire. Certains assureurs-maladie peuvent faire dépendre l'adhésion à leur assurance complémentaire de l'état de santé du demandeur. Néanmoins, le fait de poser les mêmes questions sur l'état de santé pour toutes les assurances complémentaires contrevient au principe de la proportionnalité.

Nous avons été consultés à plusieurs reprises à propos du fait que certaines assurances-maladie posent les mêmes questions pour diverses catégories d'assurances complémentaires, bien que le contenu et les prestations divergent fortement.

Lorsqu'un assureur-maladie demande des renseignements sur l'état de santé de la personne désireuse d'adhérer à l'assurance obligatoire des soins, elle contrevient à la LAMal et la LPD. Toutes les assurances-maladie sont tenues d'accepter une personne

dans l'assurance obligatoire des soins, indépendamment de son état de santé (cf. également 6e Rapport d'activités 1998/1999, p. 261).

Par contre, l'admission dans l'assurance complémentaire peut dépendre de l'état de santé de la personne qui présente une demande d'adhésion. Tout comme les autres assurances privées, les assurances complémentaires sont soumises à la loi sur le contrat d'assurance (LCA). Les assurances complémentaires sont des assurances qui offrent des prestations allant au-delà de l'assurance de base. Ainsi, les assurances complémentaires couvrent les méthodes thérapeutiques parallèles et les mesures de prévention et de promotion de la santé. Certaines assurances de voyages et de vacances couvrent aussi le coût des soins en cas de maladie ou d'accident à l'étranger. Enfin, il existe des assurances de soins dentaires couvrant des prestations que n'offrent pas les assurances obligatoires des soins. Citons par exemple les soins dentaires non opératoires, les traitements de la parodontose et les traitements en relation avec les prothèses dentaires.

Ces exemples montrent que le genre et les prestations des différentes assurances complémentaires varient considérablement. En vertu du principe de la proportionnalité, les assurances-maladie ne sont en droit de collecter que les données personnelles qui sont effectivement nécessaires et appropriées à l'assurance complémentaire en question. Ces données doivent donc être nécessaires à l'appréciation du risque lié à chaque assurance complémentaire.

Dans la pratique, on constate néanmoins d'une manière générale qu'exactement les mêmes questionnaires, en partie très détaillés, sont utilisés en vue de l'admission ou non aux diverses assurances complémentaires. Ce procédé n'est pas compatible avec le principe de la proportionnalité dont on déduit, entre autres, la règle voulant que l'on évite la collecte de données et que l'on en fasse un usage restreint. Ces principes sont d'autant plus importants qu'il s'agit dans ce cas du traitement de données médicales personnelles, donc particulièrement sensibles. On ne peut admettre que pour une assurance-voyage par exemple, il soit nécessaire de disposer des même données que pour une assurance complémentaire couvrant les soins de médecine parallèle. Pour cette raison, nous avons prié une assurance-maladie d'adapter en conséquence les formulaires de demande d'adhésion et de nous indiquer, de manière motivée, la liste des données nécessaires pour les différentes assurances complémentaires.

6.2.2. La collecte de données personnelles par les assurances-responsabilité civile

Au cours de l'année écoulée, nous avons été à de nombreuses reprises confrontés à des questions touchant le domaine des assurances-responsabilité civile. Il s'agissait pour l'essentiel de savoir quand et dans quelles conditions une assurance-responsabilité civile est en droit de collecter des données personnelles concernant les personnes lésées. Il convient dans tous les cas de tenir compte des principes figurant dans la législation sur la protection des données.

Les assurances-responsabilité civile qui cherchent à déterminer leur devoir de prestations à l'égard des personnes lésées et traitent les données personnelles de celles-ci doivent respecter les principes généraux de la protection des données (cf. également 6e Rapport d'activités 1998/99, p. 271). En particulier, une assurance-responsabilité civile ne peut, sans motif justificatif, traiter des données personnelles à l'encontre des principes généraux de la protection des données. Elle ne peut ainsi traiter des données contre la volonté expresse de la personne concernée ou communiquer à des tiers des données sensibles ou des profils de la personnalité. Une atteinte à la personnalité par une assurance-responsabilité civile n'est pas contraire au droit s'il existe un motif justificatif (le consentement du lésé, un intérêt prépondérant privé ou public, ou encore la loi). Selon la jurisprudence du Tribunal fédéral, il convient d'examiner s'il y a atteinte à la personnalité dans chaque cas d'espèce et après pesée des intérêts en jeu.

Une des questions par exemple était de savoir quand et dans quelles conditions une assurance-responsabilité civile était habilitée à demander une expertise auprès d'un psychiatre afin de pouvoir examiner la prétention du lésé. Nous avons répondu que cela nécessitait en principe le consentement de la personne lésée. Comme nous l'avons déjà mentionné, une pesée des intérêts en jeu doit être effectuée dans chaque cas. Mais tant que le consentement est possible, il ne faudrait faire appel à aucun autre motif justificatif (principe de la proportionnalité). Si la personne lésée refuse de donner son consentement ou se rétracte, l'assurance-responsabilité civile est en principe libre de ne pas entrer en matière à propos d'éventuelles exigences financières ou d'interrompre l'établissement des faits. A notre avis, un consentement est également nécessaire afin de délier le psychiatre du secret professionnel. L'expertise psychiatrique et ses résultats sont également soumis au secret professionnel en vertu du code pénal.

Dans tous les cas, les personnes lésées doivent être informées au préalable qu'une expertise va être établie. Cette obligation découle du principe de transparence et est

en accord avec le projet de révision de la loi fédérale sur la protection des données. Cette modification prévoit entre autres que la collecte de données personnelles sensibles ou de profils de la personnalité par une personne privée (comme l'assureur-responsabilité civile) doit être transparente pour les personnes concernées.

7. Secteur du travail

7.1. La communication à l'étranger de données du personnel

La communication de données du personnel à l'étranger vers des fichiers centralisés devient de plus en plus courante, surtout auprès des grands groupes d'entreprises, essentiellement dans le but de rationaliser la gestion des salaires et le recrutement du personnel.

Quatre variantes permettent de communiquer des informations via une infrastructure informatique globale. Elles se différencient essentiellement par la localisation géographique des données et par les règlements en matière de protection des données.

La première de ces variantes se caractérise par une conservation complètement centralisée des données. L'accès et le traitement des données des filiales sont réservés aux filiales autorisées et ont lieu dans le serveur central. Il n'existe dans les filiales pas de copie électronique des données centrales. Les filiales autorisées définissent les exigences dans les déclarations de traitement de données, conformément à la réglementation nationale en matière de protection des données. Cette solution est en général appliquée aux systèmes de gestion du personnel.

La deuxième variante est proche de la première. Elle s'en différencie par le fait que les données sont en principe gérées au niveau local et qu'une partie seulement d'entre elles est, selon les besoins, transférée dans le fichier central, devenant ainsi accessibles à des tiers. Le transfert de données peut avoir lieu sur demande ou de manière automatique. Par exemple, des données statistiques sur les salaires qui sont générées localement peuvent être disponibles de manière centrale afin d'être utilisées dans tout le groupe d'entreprises. Un autre exemple fréquent d'application de cette variante est la mise à disposition centralisée de données personnelles ou de profils de la personnalité des collaborateurs à des fins de recherche de personnel au sein du groupe d'entreprises même.

La troisième variante se caractérise par une stricte séparation de l'application et des données. Les données sont uniquement traitées au niveau local. Le système central d'application ne revêt qu'une fonction de liaison entre une société livrant les données (exportatrice des données) et une société recevant les données (importatrice des don-

nées). Ce système gère les déclarations de protection des données des participants et sait ainsi entre quelles sociétés l'échange de données peut avoir lieu sans problème. Les données sont ensuite directement transférées de la société exportatrice à l'importatrice après un feu vert donné par le système central d'application à la communication des données. Le système central d'application gère les adresses des systèmes participant au traitement des données et les communique à ceux-ci en cas de nécessité.

La quatrième est la variante *peer-to-peer* (d'égal à égal). Chacun des partenaires détermine lui-même les données qu'il communique ainsi que leur destinataire. Il n'existe pas ici d'instance intermédiaire. La société exportatrice des données doit décider sur la base de ses directives locales de protection des données si elle est habilitée à communiquer des données personnelles. Il n'y a pas de service central gérant les déclarations de protection des données. La manière dont les données sont communiquées est basée sur des conventions bilatérales et peuvent donc avoir lieu aussi bien sur demande que directement par procédure d'appel.

Dans chacune de ces variantes, la société importatrice des données à l'étranger devient maître du fichier de données communiquées lorsqu'elle décide du but et du contenu du fichier centralisé. A ce titre, elle est responsable de la protection et de la sécurité des données. En cas de fichier centralisé, les sociétés livrant les données sont considérées comme ayant accès aux données avec une responsabilité particulière. Elles doivent poser des conditions à la société recevant les données, pour ce qui est de la protection des données (réglementation en matière de protection des données). En 1992 déjà, le Conseil de l'Europe a établi un modèle de clause de protection des données en adoptant le contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données (cf. http://www.edsb.ch/f/gesetz/europarat/mustervertrag.htm).

Pour ce qui est de la communication de données de l'entreprise importatrice des données à des entreprises tierces, la Commission des Communautés européennes a, dans sa décision du 15 juin 2001, établi des conditions claires quant aux clauses des contrats-types prévoyant la communication de données relatives à des personnes dans des pays tiers. (cf. http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_fr.pdf).

Le but de la communication des données à l'étranger doit reposer sur un motif justificatif conformément à l'art. 13 LPD. La rationalisation de la gestion des salaires et du recrutement du personnel est considérée comme motif justificatif. Néanmoins, seules les données personnelles nécessaires à l'accomplissement du but peuvent être transmises.

Lorsqu'une société importatrice de données communique des données à des entreprises dans des Etats tiers, elle doit se renseigner tout d'abord pour savoir si ces Etats disposent d'une protection des données équivalente à celle pratiquée en Suisse. Si tel n'est pas le cas, la protection des données avec ces entreprises doit être garantie par contrat. Cette obligation est particulièrement importante lors de la création de pools de données destinés à pourvoir à un poste à l'intérieur du groupe d'entreprises.

S'il confie le traitement des données à un tiers, le mandant doit veiller à ce que ne soient pas effectués des traitements autres que ceux qu'il est lui-même en droit d'effectuer et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Les données personnelles transmises doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles adéquates. Il est donc recommandé de prendre des mesures de protection spécifiques selon la classification des catégories de données. L'impossibilité d'accéder sans autorisation à l'infrastructure de communication et aux supports de données doit être en permanence garantie. De même, le cryptage des données doit permettre d'en interdire l'accès aux personnes non autorisées. Il doit répondre aux dernières connaissances techniques en la matière. Cela vaut à la fois pour les données et pour les déclarations de protection des données. L'identification des personnes autorisées à recevoir les données conformément aux déclarations doit être clairement garantie. Elle doit répondre aux dernières connaissances techniques en la matière et faire l'objet d'une journalisation pour que l'on puisse en tout temps retracer le traitement des données.

7.2. Conservation des dossiers du personnel

Après l'établissement d'un dossier personnel, un devoir de conservation incombe à l'employeur. Ce devoir diffère selon les dossiers personnels et la date de leur établissement. La durée de conservation commence au moment de l'établissement du dossier personnel, et non pas à la fin des rapports de travail.

Conservation des données relatives au salaire

La personne à qui incombe la tenue des livres doit les conserver, ainsi que la correspondance commerciale et les pièces comptables, durant dix ans. Le délai de conservation commence à la fin de l'année civile au cours de laquelle les dernières inscriptions ont été effectuées ou durant laquelle les dernières pièces ont été soit envoyées, soit versées au dossier. L'ordonnance du 2 juin 1976 concernant l'enregistrement des documents à conserver règle les détails, en particulier la responsabilité de la conservati-

on. La comptabilité des salaires, y compris toutes les données pertinentes concernant ceux-ci, fait partie des livres.

Données nécessaires à l'établissement du certificat de travail

Le délai de prescription de dix ans prévu par l'art. 127 CO est également valable, selon l'opinion dominante, pour le droit à l'établissement, à la justification, à la correction ou au complément d'un certificat de travail. Il est possible de faire valoir ces droits jusqu'à dix ans après la fin des rapports de travail. Le devoir de conservation de l'employeur concerne surtout les données sur le genre et la durée du rapport de travail, la description des tâches et le domaine de responsabilité, les appréciations de la prestation fournie, du comportement et de la gestion, la carrière et la formation continue, les motifs du départ ainsi que les données sur des événements particuliers. Ces données se trouvent essentiellement dans le cahier des charges, dans les entretiens d'appréciation des collaborateurs, dans le plan de carrière et dans les documents concernant la poursuite de la formation professionnelle. Seules les deux dernières appréciations des collaborateurs sont en général utiles à l'établissement du certificat de travail. Les appréciations précédentes doivent être régulièrement enlevées du dossier personnel et détruites.

Documents qui appartiennent aux travailleurs

Les dossiers de candidature, comprenant par exemple le curriculum vitae, les certificats de travail précédents, les diplômes, les exemples de travaux, les photos et les autres documents qui appartiennent à l'employé et pour lesquels l'employeur n'a aucun intérêt légitime à les conserver doivent être rendus au plus tard à la fin du rapport de travail. La remise de ces documents se fait néanmoins généralement dès la fin de la période d'essai.

Documents qui appartiennent à l'employeur

Les documents appartenant à l'employeur, mais pour lesquels il n'a toutefois plus d'intérêt légitime à les garder doivent être détruits au plus tard à la fin du rapport de travail. L'employeur peut également les rendre à son employé. Il s'agit ici tout particulièrement d'anciens documents relatifs aux qualifications de l'employé qui ne sont plus nécessaires à l'établissement et à la motivation du certificat de travail, mais également les expertises graphologiques, psychologiques ou médicales ainsi que des tests psychologiques. Ces documents également devraient être rendus ou détruits un à deux ans déjà après leur établissement.

Remarques générales

La durée de conservation dépendant de la date à laquelle le dossier personnel a été établi, nous recommandons de faire figurer de manière lisible sur chaque pièce du dossier la date d'établissement de celui-ci ainsi que la durée de conservation. Cela facilitera le contrôle de la date limite de conservation ainsi que le triage régulier des documents composant le dossier.

Les données personnelles ne peuvent être conservées plus longtemps, en dérogation aux règles mentionnées ci-dessus, qu'avec le consentement de l'employé et uniquement à son avantage.

S'il y a des litiges en cours, l'employeur conservera toutes les pièces dont il a besoin comme moyen de preuve jusqu'au règlement du litige. Par exemple au cas où un employé ferait valoir l'un des droits mentionnés plus haut juste avant l'expiration du délai de prescription de dix ans, l'employeur peut conserver les moyens de preuve nécessaires jusqu'au règlement du litige, c'est-à-dire jusqu'à l'écoulement des délais de recours prévus. La durée de conservation des moyens de preuve nécessaires peut donc être étendue au-delà du délai de prescription de dix ans.

7.3. La communication de données personnelles dans le cadre des conventions collectives de travail

Lorsque la convention collective de travail prévoit le contrôle des dispositions relatives aux salaires et de ce fait la communication des données concernant les salaires, on considère qu'il y a eu consentement des parties au contrat. Le juge doit décider en l'espèce s'il existe des motifs justificatifs autres que le consentement des employés pour qu'il puisse y avoir communication des données. Il est souhaitable à ce propos que le législateur crée un organe indépendant de contrôle.

Une convention collective de travail (CCT) peut prévoir le contrôle de ses dispositions sur les salaires par une commission paritaire, composée de représentants des employeurs et des travailleurs. En outre, les données concernant les salaires des employés peuvent être transmises à cette commission.

Conformément à l'article 328b du code des obligations, l'employeur ne peut traiter et transmettre les données concernant les travailleurs que si elles portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. Il ne peut être dérogé à cette disposition qu'en faveur des travailleurs (art. 362 CO).

Un employeur ne peut traiter et transmettre des données que s'il existe un motif justificatif (art. 12., al. 1 et art. 13, al. 1 LPD). Une loi, le consentement de la personne concernée ou un intérêt prépondérant public ou privé peuvent constituer un motif justificatif.

Il n'existe pas de base légale prévoyant la transmission des données à une commission paritaire. Les seuls motifs justificatifs possibles sont donc le consentement de la personne concernée et un intérêt prépondérant public ou privé.

Lorsque le contrôle des dispositions relatives aux salaires et de ce fait la transmission des données les concernant sont prévues dans la CCT, cela équivaut à un consentement des parties contractantes. En général, tous les travailleurs adhèrent à la CCT soit directement, soit par représentation. De ce fait, les travailleurs qui ne sont pas soumis à la CCT doivent être informés au préalable de la possibilité de communiquer des données les concernant et doivent y consentir expressément.

Il appartient au juge d'établir s'il y a un intérêt prépondérant public ou privé à la transmission des données concernant le salaire ou si cette transmission est dans l'intérêt du travailleur. Il paraît néanmoins plausible que le travailleur en tant que partie contractante à la CCT a un intérêt à ce que les dispositions relatives aux salaires soient respectées.

La transmission des données relatives aux salaires par une publication générale de la comptabilité du personnel n'est toutefois pas autorisée car cette comptabilité contient également des données sur des tiers.

Il est possible d'élargir le domaine de validité de la CCT à des employeurs et des travailleurs qui ne sont pas liés par cette convention et qui peuvent demander à l'autorité cantonale compétente la désignation d'un organe de contrôle indépendant. L'autorité détermine l'objet et l'ampleur du contrôle après avoir entendu d'une part les parties à la CCT et d'autre part les employeurs ou les travailleurs qui demandent la désignation de l'organe de contrôle spécial (art. 6 de la loi fédérale du 28 septembre 1956 permettant d'étendre le champ d'application de la convention collective de travail).

Il est souhaitable que le législateur prévoie expressément cette possibilité pour toutes les CCT étant donné qu'avec cette réglementation, les membres de l'organe de contrôle sont indépendants des deux parties contractantes et donc pas confrontés à un conflit d'intérêts.

7.4. Surveillance des communications téléphoniques sur le lieu de travail (call centers)

Deux personnes conversant au téléphone doivent être informées au préalable de l'écoute ou de l'enregistrement et y donner leur consentement. Une information unique dans le contrat suffit lorsque les écoutes ou les enregistrements ont lieu de manière systématique. Par contre, s'ils sont occasionnels, il faut en informer les personnes concernées avant chaque entretien téléphonique.

Le code pénal requiert le consentement des deux interlocuteurs au cas où les conversations téléphoniques seraient écoutées ou enregistrées. Le contenu des conversations téléphoniques ne doit être enregistré que pour des motifs de contrôle des prestations (par ex. contrôle de qualité en cas de vente par téléphone, but de formation) ou pour des raisons de sécurité (par ex. conservation des preuves). L'écoute ou l'enregistrement est autorisé lorsque tous les interlocuteurs enregistrés ou écoutés ont au préalable donné leur consentement et ont été informés sans ambiguïté et en temps voulu.

Il n'est pas absolument nécessaire d'informer de l'écoute ou de l'enregistrement à chaque conversation lorsque ces écoutes ou ces enregistrements sont effectués systématiquement et que tous les interlocuteurs en ont été auparavant informés de manière claire. Cette solution est par exemple envisageable dans certains secteurs bancaires où l'on traite des affaires juridiques par téléphone. Dans de tels cas, une information expresse préalable figurant dans le contrat de travail suffit pour l'employé; pour la clientèle, cette information se fera dans les conditions générales. On peut également envisager des situations où les employés reçoivent une information unique, dans le contrat de travail, et où par contre tous les clients sont informés par une bande enregistrée. Il peut également arriver que les clients informés contractuellement (conditions générales) tout comme des personnes non liées contractuellement participent à l'entretien téléphonique. Les premiers seront informés dans les conditions générales, les seconds le seront oralement.

Les écoutes et les enregistrements occasionnels de conversations avec des tiers sont par exemple envisageables dans le cadre d'un service de renseignements (call centers). Les employés sont, en général, informés qu'ils sont mis sur écoute ou enregistrés à chaque conversation par un signal optique ou acoustique. Afin de mieux satisfaire aux intérêts de l'employeur, notamment pour ce qui est de l'efficacité de la formation, il est compatible avec la protection de la personnalité que les employés ne soient informés que de la période choisie de mise sur écoute ou d'enregistrement. Cette période ne doit pas dépasser cinq jours, pour des raisons de proportionnalité et de

protection de la personnalité et de la santé. Le devoir d'information des autres interlocuteurs demeure évident et a lieu en général par une bande enregistrée.

7.5. L'établissement de dossiers secrets dans le domaine du travail

Le dossier personnel d'un employé comprenant des notes écrites et des pièces personnelles n'est pas considéré comme un traitement de données destiné à l'usage exclusivement personnel de l'employeur. De ce fait, il est soumis à la loi sur la protection des données, notamment pour ce qui est du droit d'accès.

La constitution de dossiers auxquels les employés n'ont pas accès (dossiers secrets) et la destruction de données personnelles en contradiction avec les principes de la protection des données, notamment avec le principe de la proportionnalité dans le cadre de la durée de conservation, lèse les droits de la personnalité des employés. Le premier droit concerné est le droit d'accès à des informations dissimulées aux employés en raison de leur caractère critique. Par voie de conséquence, le droit de rectification et le droit de contestation (droit de réponse) se trouvent également entravés. L'employeur peut certes refuser ou restreindre le droit d'accès, voire en différer l'octroi si des intérêts prépondérants privés ou publics l'exigent. La LPD oblige néanmoins le maître du fichier à indiquer le motif pour lequel il refuse de fournir, limite ou ajourne les renseignements. L'indication de ce motif doit permettre d'une part aux personnes concernées de vérifier l'admissibilité et la validité de la restriction et d'autre part, au juge de saisir les motifs principaux à la base de la décision du maître du fichier. Il convient de souligner à ce propos que les notes personnelles de l'employeur qui ne sont pas communiquées à des personnes extérieures ne sont pas soumises au droit d'accès. Il s'agit par exemple des notes que quelqu'un prend certes dans l'exercice de sa profession, mais en tant qu'aide-mémoire ou référence destinés uniquement à son usage personnel, notamment dans le but de disposer d'un instrument de travail personnel. Cette disposition ne doit en aucun cas être invoquée par la personne traitant les données afin de contourner les prescriptions de la LPD. Les données traitées au départ pour un usage personnel tombent sous le coup de la LPD dès qu'elles sont communiquées à une tierce personne. Dans le domaine professionnel, cette communication englobe également la communication des données à l'intérieur de l'entreprise. Ainsi, transmettre des données par exemple entre collègues de travail se traduit par l'exclusion de l'exception et mène à l'application de la LPD.

L'établissement de dossiers secrets va également à l'encontre du principe de la bonne foi selon lequel les employés peuvent légitimement se fier à leur employeur pour qu'il les informe des traitements de données les concernant. Quiconque rassemble des

données en cachette se heurte à ce principe même s'il ne viole pas une norme juridique. L'exigence selon laquelle la collecte de données doit être transparente pour la personne concernée, à savoir non dissimulée, découle de ce principe.

En cas de violation du droit d'accès et du principe de la bonne foi, les employés concernés peuvent non seulement faire valoir des prétentions de droit civil (rectification, destruction ou blocage de données personnelles), le cas échéant liées à des demandes de dommages-intérêts ou de sanctions, mais ils disposent aussi de moyens de droit pénal. Le tribunal des prud'hommes traite les prétentions de droit civil. Il statue en général au cours d'une procédure rapide et gratuite. Pour ce qui est des affaires de droit pénal, le juge compétent est désigné par le code cantonal de procédure pénale.

Ces réflexions sur le droit d'accès et le principe de la bonne foi valent également pour ce qui est de la collecte d'informations. Les employés ont le droit d'être informés de l'origine des données rassemblées. Dans certains cas, l'employeur est néanmoins tenu pour des raisons de protection de la personnalité de taire l'identité des personnes ayant fourni les renseignements si leurs intérêts en matière de protection de la personnalité sont prépondérants. On peut imaginer par exemple que l'employeur donne comme source des renseignements l'ensemble des collaborateurs ou des groupes de collaborateurs sans faire le lien entre les collaborateurs et certaines informations ou déclarations.

7.6. Violation du devoir de discrétion par des bureaux de placement privés

Les bureaux de placement privés ne peuvent communiquer des données sur des demandeurs d'emploi aux offices régionaux de placement (OFP) que si la personne concernée y a donné son consentement.

Les bureaux de placement privés ne peuvent traiter les données concernant les demandeurs d'emploi et les places vacantes que si le placement de la personne le requiert et aussi longtemps que cela est nécessaire. La communication de données est réglée de manière exhaustive dans la législation correspondante. Il n'existe pas de base légale réglant la communication de données, sur un demandeur d'emploi, d'un bureau privé de placement aux offices régionaux de placement. Le devoir de discrétion est ici applicable. Conformément à la loi sur la protection des données, la personne concernée a le droit d'exiger une décision constatant le caractère illicite du traitement effectué. Le devoir de discrétion disparaît lorsqu'un demandeur d'emploi a autorisé par écrit la communication de ses données.

7.7. Contrôle de l'employeur durant l'absence

L'employeur n'est en droit de contrôler le comportement d'un employé absent pour raison de maladie que pour s'informer de manière générale et uniquement en cas de soupçon concret d'un comportement contraire au contrat.

Un syndicat nous a exposé les faits suivants: pour des raisons de santé, un employé avait été mis en congé de maladie durant un certain temps. L'incapacité de travail concernait l'accomplissement d'activités corporelles. L'employé avait informé son employeur de la maladie et de sa durée, mais avait omis de dire qu'il avait effectué durant cette période et pendant toute une journée un travail purement intellectuel auprès d'un second employeur. L'employeur, qui savait que son employé avait un second métier, se renseigna auprès du second employeur au sujet des activités éventuelles de son employé durant le congé de maladie de celui-ci. Il n'y avait aucun indice concret de comportement contraire au contrat. Le second employeur confirma la présence de l'employé durant une journée, suite à quoi le premier employeur prit des mesures contre son employé. Il les motiva par la violation du devoir découlant de la convention collective de travail selon lequel l'employeur doit être informé des longues absences de l'employé de son domicile. Le syndicat de l'employé s'est adressé à nous pour savoir si un contrôle de cette sorte était légal. Nous sommes parvenus à la conclusion exposée ci-dessous.

L'employeur se doit de protéger et de respecter la personnalité de ses employés. Il ne doit en particulier traiter les données sur les employés que si elles portent sur l'aptitude de l'employé à remplir son emploi ou si elles sont nécessaires à l'exécution du contrat de travail. Les données concernant la sphère privée qui n'ont aucun lien avec le rapport de travail ne doivent pas être traitées. Par ailleurs, l'employeur doit traiter les données selon le principe de la bonne foi. Cela signifie que les employés doivent en être généralement informés auparavant.

Les employés se doivent d'exécuter les tâches qui leur incombent de manière scrupuleuse et de défendre les intérêts légitimes de l'employeur en toute loyauté. Pendant la durée du rapport de travail, les employés ne peuvent notamment fournir de travail rémunéré pour des tiers dans la mesure où cette activité contrevient à leur devoir de loyauté, notamment où elle concurrence l'employeur. Celui-ci peut établir des dispositions générales sur l'exécution du travail et le comportement des employés dans l'entreprise ainsi que leur donner des instructions particulières. Les employés doivent s'y conformer en toute bonne foi.

En matière de surveillance du comportement des employés, il est extrêmement im-

portant de les informer que le respect des obligations contractuelles peut être contrôlé. Ce point découle du principe de la bonne foi. Sans information préalable, les employés sont en droit de supposer que le rapport de travail est basé sur la confiance, respectueux de la personnalité et qu'ils ne sont pas surveillés. En outre, la surveillance suppose l'existence d'indices de suspicion d'un comportement contraire au contrat. Si tel n'était pas le cas, il y aurait un risque de contrôles arbitraires par l'employeur. Si l'une de ces conditions n'est pas remplie, il n'est pas permis de contrôler le comportement de l'employé durant son congé de maladie.

Dans le cas présent, ni l'interdiction de concurrence, ni le devoir de loyauté n'ont été transgressés du fait que l'activité exercée durant le congé de maladie n'était pas de nature corporelle, mais de nature intellectuelle et que l'employeur était au courant du second rapport de travail de son employé et n'y avait formulé aucune objection. De même, la disposition prévue par la convention collective de travail sur l'obligation d'annoncer toute absence prolongée du domicile n'avait pas été violée puisque l'activité exercée n'avait pas dépassé la durée d'une journée. Il n'y avait donc pas eu de comportement contraire au contrat. L'employeur n'avait pas non plus informé ses employés de la possibilité de tels contrôles.

7.8. Dépistage de la consommation de drogues chez les apprentis: transmission de la recommandation à la Commission fédérale de la protection des données

Comme nous l'avions déjà mentionné dans notre 8e Rapport d'activités 2000/2001 (p. 146), le groupe Hoffmann-La Roche a rejeté notre recommandation en matière de test de dépistage de la consommation de drogues chez les apprentis. Nous avons porté l'affaire devant la Commission fédérale de la protection des données pour décision. Notre mémoire figure en annexe p. 132.

7.9 Règlement-type régissant la surveillance du courrier électronique et de l'utilisation d'Internet sur le lieu de travail

Après la parution du guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail, nous avons publié à ce propos un règlement-type (cf. p. 114). Il a été conçu pour les entreprises qui désirent établir un règlement pour l'utilisation et la surveillance d'Internet et du courrier électronique sur le lieu de travail.

7.10. Ordonnance concernant la protection des données personnelles dans l'administration fédérale

Le 3 juillet 2001, le Conseil fédéral a adopté l'ordonnance concernant la protection des données personnelles dans l'administration fédérale sans que nos préoccupations transmises au cours de la procédure de co-rapport aient été prises en considération. L'ordonnance est entrée en vigueur le 1er janvier 2002.

Le 24 mars 2000, l'Assemblée fédérale a adopté la loi sur le personnel de l'administration fédérale. Cette loi est entrée en vigueur le 1er janvier 2001 pour les CFF et le 1er janvier 2002 pour l'administration fédérale et la Poste. Une ordonnance d'exécution règle le traitement des données personnelles des employés, des anciens employés ainsi que des candidats à des postes de l'administration fédérale. L'ordonnance prévoit entre autres le dépôt dans le dossier personnel d'une copie du formulaire d'appréciation. Nous avons précisé dans le cadre de la procédure de co-rapport que les appréciations personnelles ne doivent en aucun cas être consultables dans leur totalité par le service du personnel. En effet, un service du personnel n'a pas besoin pour remplir sa tâche (par ex. fixer le salaire, organiser des cours de formation continue) de l'appréciation globale ainsi qu'éventuellement d'autres données d'ordre organisationnel. Ces informations peuvent être aisément portées à la connaissance du service du personnel à l'aide d'un document séparé. C'est pour cette raison que nous avons recommandé d'adapter dans ce sens le projet d'ordonnance et de renoncer à l'adjonction systématique d'une copie du formulaire d'appréciation. La seule possibilité entrant en ligne de compte est l'adjonction au dossier d'une copie dans une enveloppe fermée. Le service du personnel ne devrait consulter le formulaire d'accompagnement que dans des cas d'espèce fondés. Notre argumentation n'a toutefois pas été prise en considération.

8. Economie et commerce

8.1. Exigences générales visant la vérification des sites Web (labels de qualité)

La multiplication des processus commerciaux basés sur Internet (commerce électronique) place les entreprises face à de nouveaux défis. Une question en particulier mérite un examen plus approfondi: les risques que représente l'utilisation des nouvelles technologies pour la sphère privée.

L'utilisation de nouvelles technologies comporte des risques spécifiques. La mise en

réseaux des systèmes concerne à la fois le flux de données de toute une entreprise et les processus commerciaux conventionnels. L'image que donne l'entreprise quant à la sécurité des données est essentielle. En effet, un manque de confiance de la part des partenaires commerciaux et des clients potentiels est à même de mettre en péril la réussite de cette entreprise en matière de commerce électronique.

L'introduction d'un label de qualité et sa vérification dans le cadre d'une révision informatique par un organisme indépendant donne à l'entreprise la possibilité de faire état de ses normes en matière de sécurité et de protection des données.

Il convient à cet effet de tenir compte des éléments suivants:

- sécurité de l'accès aux données,
- protection des données personnelles,
- confidentialité des données,
- disponibilité des données,
- intégrité des données.

Il est important à cet égard que les critères de vérification répondent à des règles uniformes au niveau international et soient publiés sur Internet afin que la norme de qualité puisse être identifiée de manière objective. La vérification doit être planifiée et effectuée conformément à des normes de vérification reconnues. L'attribution du label de qualité doit émaner uniquement d'organismes d'audit reconnus qui doivent être indépendants des entreprises. Pour de plus amples informations sur les labels de qualité, se reporter au 8e Rapport d'activités 2000/2001, p. 144.

8.2. Publicités non désirées par courrier électronique (spam)

Les campagnes de publicité par courrier électronique en masse (spam) ne cessent de s'intensifier. Notre législation est encore insuffisante pour faire face au harcèlement publicitaire qu'est le spam. Deux affaires nous ont plus particulièrement occupés ces derniers mois. La première a trait à la commercialisation d'un CD-ROM contenant les données personnelles de plus d'un demi- million de personnes résidant en Suisse et la seconde concerne l'envoi répété et massif de publicités non désirés par e-mail en provenance d'une personne domiciliée à Zürich.

La législation suisse consacre le principe dit de «l'opt-out» (par opposition au principe dit de «l'opt-in»). Cela signifie que la publicité par e-mail est par principe admise, sauf en cas de refus exprès du destinataire. La Suisse est en train de revoir sa législation

afin de la rendre plus contraignante à l'encontre des publicités non désirées adressées par la voie du e-mail. De son côté, l'Union européenne est en train de mettre sur pied une législation dans ce domaine, qui devrait s'orienter vers la solution de l'opt-in. Au niveau européen, ce principe est déjà devenu obligatoire pour la publicité par appels téléphoniques avec sélection automatique et par voie de SMS.

Affaire du CD-ROM Black Book 2000

Il s'agit d'un CD-ROM baptisé «Black Book 2000» produit aux USA et commercialisé en Suisse. Grâce à plusieurs tabelles de présélection, celui-ci donnait accès aux noms, prénom, profession, adresse e-mail et postale d'environ 500'000 personnes résidant en Suisse. Après enquête, nous avons pu constater que ces données n'avaient pas toujours été collectées de manière licite. Des adresses e-mail ont notamment été extraites de la banque de données des enregistrements Switch (contrairement aux finalités explicites de cette dernière). D'autres adresses e-mail ont été tirées du site Internet d'une personne ayant expressément exclu son utilisation à des fins publicitaires. Enfin, certaines données personnelles ont été collectées, alors même que la personne s'y était publiquement opposée (par une inscription sur la liste Robinson ou en faisant recours à la mention de l'étoile dans l'annuaire téléphonique). Par ailleurs, le CD-ROM faisait figurer la mention «opt-in» aux côtés des données, alors même que le consentement exprès des personnes concernées n'avait pas été obtenu en amont. De surcroît, le CD-ROM comportait une multitude de données personnelles fausses, ce qui contrevient au principe de l'exactitude des données. Le diffuseur du CD-ROM en Suisse a considéré pour sa part, qu'il n'y avait pas de collecte illicite. Selon lui, les données en cause avait été réunies à partir de différents espaces publics (site Internet et forum de discussion). De plus, lesdites données avaient été réunies grâce à l'utilisation d'un moteur de recherche particulier. Celui-ci était soit disant capable de repérer le refus d'une personne quant à l'utilisation de ses données personnelles à condition que ladite personne ait exprimé ce refus par Metatags (programmation dans le code source). En outre, le moteur de recherche en question était standard pour la communauté des utilisateurs d'Internet. Enfin, il est précisé sur le CD-ROM lui-même qu'il ne doit pas servir d'instrument de spam.

Bien que l'activité de spam n'ait pu être démontrée, nous avons estimé que le CD-ROM n'était pas conforme à la législation suisse sur la protection des données. Dans notre recommandation adressée au vendeur dudit CD-ROM en Suisse, nous avons demandé qu'il ne soit plus commercialisé dans sa version actuelle, que les données collectées de manière illicite soient supprimées dans la prochaine version, que les droits des personnes concernées soient respectés (suppression de leur données lorsqu'elles en ont fait la demande), que les inexactitudes (mention de l'opt-in et données fausses)

soient supprimées et enfin, qu'il soit donné suite au droit d'accès. Voir également notre recommandation p. 132.

Affaire de la vente d'articles par spam

Depuis des années, une personne domiciliée à Zürich entreprend régulièrement des campagnes de publicité par e-mail pour différents produits. Les e-mails contiennent un talon-réponse où figure son adresse pour les commandes. En revanche l'identité de l'expéditeur du spam lui-même n'apparaît jamais clairement. Cependant, il ne fait nul doute qu'il s'agit de la même personne, celle-ci n'ayant jamais nié son rôle dans l'expédition desdites publicités (le spammeur). Or lorsqu'une personne destinataire d'un tel spam exerce son droit d'accès, le spammeur refuse d'y donner suite. Il considère, en effet, que les adresses e-mail ne sont pas des données personnelles et qu'en conséquence, ses publicités ne tombent pas sous le coup de la loi. Nous avons réaffirmé que l'utilisation d'adresses e-mail représente un traitement de données personnelles tombant sous le coup de la loi sur la protection des données. De plus, les adresses e-mail constituent des données personnelles, y compris en cas d'utilisation d'un pseudonyme. En effet, une adresse e-mail se rapporte nécessairement à une personne donnée qui, si elle n'est pas immédiatement identifiée, reste pour le moins identifiable. Nous avons demandé au spammeur de garantir les droits des personnes concernées à savoir de supprimer de son fichier d'adresses leurs données personnelles et de permettre l'exercice du droit d'accès.

9. Finances

9.1. Communication de données personnelles extraites de demandes d'ouverture de comptes

Une banque promet à ses clients, dans les demandes d'ouverture de compte, que ceux-ci peuvent révoquer en tout temps leur consentement au traitement de données. Or chaque fois qu'un futur client exprime une demande dans ce sens, la banque refuse immédiatement de conclure le contrat. Par ailleurs, elle ne veut pas divulguer à qui elle transmet les données personnelles collectées de cette manière. Nous avons rendu, contre cette pratique, une recommandation que la banque a acceptée. Le texte de cette recommandation est reproduit à la page 132.

Une banque appartenant à un grand groupe d'assurances offre diverses formes de placements financiers. Les personnes qui s'y intéressaient recevaient généralement de la banque des formulaires de demande d'ouverture de compte pour les différents

genres de placement. Dans les conditions générales figurant sur ces formulaires de demande, on trouvait entre autres la rubrique «Traitement de données». Il y était dit textuellement: «Le consentement au traitement des données peut être révoqué en tout temps». La banque répondait aux personnes qui se prononçaient contre ce traitement de données que, dans ces conditions, aucun contrat ne pouvait être conclu. De nombreuses personnes se sont adressées à nous pour demander conseil.

En 1999 déjà, nous étions intervenus auprès de cette banque non seulement en raison de cette clause de consentement équivoque, mais nous nous sommes également prononcés contre le fait que la désignation imprécise «aux sociétés appartenant au X Services Group» soit utilisée comme éventuel destinataire ultérieur des données. Ce n'est qu'après de nombreux courriers que la banque se déclara prête, en automne 1999, à renoncer à cette clause de consentement prêtant à confusion et donna à ses clients la possibilité de demander à la banque une liste des sociétés appartenant au X Services Group. La banque promit d'adapter immédiatement en conséquence la rubrique «Traitement de données».

Au printemps 2001, force nous a été de constater à plusieurs reprises que la banque, contrairement à ses engagements, utilisait encore les formulaires de demande d'ouverture de compte comportant le texte initial. Nous l'avons contactée à ce sujet et elle promit à nouveau d'abandonner immédiatement la clause de consentement en question. Elle nous informa en même temps de sa décision de ne pas fournir à ses clients la liste des entreprises auxquelles elle transmettait les données personnelles. Lorsque quelques semaines plus tard, des demandes d'ouverture de compte sur lesquelles figurait toujours le même texte nous furent remises, nous nous sommes de nouveau adressés à la banque et avons, à cette occasion, attiré une fois de plus son attention sur le fait que le refus de remettre une liste de toutes les sociétés appartenant au X Services Group contrevenait à divers égards au droit de la protection des données.

Nous avons expliqué à la banque qu'un particulier ne sachant pas exactement à qui ses données personnelles vont être transmises ne peut librement décider s'il accepte que ces données soient effectivement transmises et à qui. Cette absence d'information va à l'encontre du droit à l'autodétermination individuelle en matière d'information. En outre, la banque se méprenait sur le fait qu'en tant que principe fondamental du droit de la protection des données, le principe de la transparence doit être respecté sans restriction dès le moment où commence le traitement de données personnelles et non pas seulement au moment où une information est éventuellement demandée. La banque a accepté notre recommandation dans ce sens.

10. Statistique et recherche

10.1. Mise en œuvre du recensement de la population 2000

Depuis le 5 décembre 2000, nos activités de contrôle ont porté sur les traitements des données du recensement de la population 2000 suivants: plausibilité, complétude, enquête de couverture, retour des données dans les cantons aux fins d'harmonisation, anonymisation et destruction des données.

Le cadre légal, la pré-impression des questionnaires du recensement 2000, l'activité du centre de services DCL, celle du groupe de contrôle cantons/Confédération, ainsi que nos premières visites en différents lieux de traitement des données ont été décrits dans les précédents rapports d'activités (5e Rapport d'activités 1997/1998, p. 206, 6e Rapport d'activités 1998/1999, p. 303., 7e Rapport d'activités 1999/2000, p. 193, et 8e Rapport d'activités 2000/2001, p. 179).

La suite de notre activité de contrôle s'est effectué à l'Office fédéral de la statistique (OFS), au centre de services DCL et au call center exploité par la société Demoscope AG.

OFS

L'OFS dispose, pour des raisons liées au contrôle de la production et du développement du projet, d'un accès à la banque de données du centre de services DCL. En mars 2001, nous avons effectué la visite de ces installations et avons pu constater qu'elles sont séparées physiquement du réseau informatique de l'OFS. En outre, les données auxquelles l'OFS a accès dans ce cadre sont anonymisées. Ainsi, nous avons estimé que ces mesures étaient à même de garantir la protection des données.

DCL

En avril 2001, nous sommes retournés inspecter le fonctionnement des installations et le travail effectué au centre de services DCL. Nous avons demandé d'améliorer la journalisation, notamment pour les personnes qui disposent d'un accès privilégié. Pour le reste, un bilan intermédiaire a été établi et nous avons jugé, avec l'organe de contrôle extérieur, que la possibilité d'abus était très restreinte au vu des moyens mis en place pour la protection des données.

e-census

Environ 4% de la population a utilisé le système e-census, lequel donnait pour la première fois la possibilité de remplir les questionnaires du recensement et de le transférer via Internet. Un règlement de traitement a été élaboré et un audit de ce système a été effectué par une entreprise extérieure. Peu après sa mise en route, ledit système

s'est bloqué pour cause de surcharge du réseau. Ce dysfonctionnement a eu pour conséquence que l'accès au système n'était plus donné. Cette panne n'a pas duré longtemps et ne s'est pas reproduite. Fin mars 2001, le système a été déconnecté du réseau Internet sous la surveillance de l'Unité de stratégie informatique de la Confédération et de l'organe de contrôle extérieur. De manière générale, nous n'avons pas enregistré d'anomalies susceptibles de mettre en danger la protection des données.

Plausibilité et complétude

En avril 2001, nos représentants ont visité les installations du call center de la société Demoscope AG chargé de collecter par téléphone les indications manquantes et de corriger les données non plausibles des questionnaires du recensement 2000. Nous avons estimé que les mesures adéquates avaient été prises afin de garantir les opérations en question. Celles-ci ont débuté peu après pour s'achever à la mi-octobre 2001.

Enquête de couverture

Pour la première fois, la législation suisse a prévu la réalisation, après le recensement, d'une enquête de couverture visant à contrôler la qualité des données obtenues. L'OFS a confié cette tâche à la société IHA GfM. Cette enquête a été soumise aux prescriptions de protection des données valant pour le recensement. Elle a été effectuée, essentiellement par téléphone et sur un échantillon de 27'000 ménages (environ 60'000 personnes).

Démarchage téléphonique et protection des données

Certaines personnes sollicitées au téléphone par IHA GfM ou Demoscope AG, se sont adressées à notre secrétariat, afin de savoir si les enquêtes téléphoniques décrites plus haut (complétude/plausibilité et enquête de couverture) étaient officielles et légales. Ces personnes souhaitaient en particulier connaître les moyens de se préserver des imposteurs. A cet égard, une hot-line a été mise sur pied par l'OFS dans le but de répondre aux questions de cette nature. Afin de se légitimer, tous les opérateurs ont reçu des consignes très précises en rapport avec leur façon de s'annoncer. Ils devaient notamment donner leur nom, le nom de leur entreprise et expliquer leur mandat par rapport à l'OFS. Dans les cas où un doute subsistait, l'OFS a procédé à un contrôle permettant de remonter à l'heure du téléphone en cause et de vérifier si c'était effectivement un employé qui avait effectué le téléphone mis en cause. L'ayant nous-même testé, nous avons jugé que le système mis en place était suffisant.

Anonymisation et destruction des données du recensement 2000

Aux termes de la loi fédérale sur le recensement de la population, la mise à jour des registres cantonaux et communaux doit avoir lieu dans les six mois qui suivent la fin de

la collecte. L'établissement du registre fédéral des bâtiments et de logements doit être achevé au moment où les données sont apurées.

D'après les informations dont nous disposons, la fin du relevé correspond à la fin de l'année 2001 (fin de la procédure de rappels). L'anonymisation et la destruction des données du recensement 2000 doivent ainsi intervenir dans l'intervalle et en tout cas dès que le but du traitement a été atteint. Un concept de destruction et d'anonymisation des données figure dans le règlement de traitement du recensement 2000.

L'organe de contrôle extérieur nous a transmis plusieurs attestations confirmant la destruction des données en possession des entreprises actives dans la pré-impression des questionnaires. Il en va de même pour les données en possession de la société Bee company (hot-line en fonction lors du recensement, cf. 8e Rapport d'activités 2000/2001, p. 179) et des données détenues par la société Demoscope AG. La destruction des données en main de IHA GfM n'a pas encore débuté eu égard au fait que l'enquête de couverture s'achèvera courant 2002 et que l'appariement des données collectées dans ce cadre avec celles du recensement doit encore avoir lieu.

Nous devons, par conséquent, encore veiller à ce que le concept d'anonymisation et de destruction des données se fasse correctement et dans les délais prévus par la loi.

Retour des données dans les cantons et communes aux fins d'harmonisation

Le retour des données du recensement 2000 aux cantons et communes aux fins d'harmonisation des registres a commencé à fin 2001 Aucune sanction ne peut être infligée à une personne dans le cadre de cette actualisation des fichiers cantonaux et communaux. Le contrôle du système mis en place pour le retour des données en vue d'harmoniser les registres cantonaux et communaux a été effectué par l'organe de contrôle extérieur et le contrôle du traitement des données du recensement 2000 par les organes cantonaux et communaux incombe aux autorités cantonales compétentes.

10.2. Harmonisation des registres de personnes

La nouvelle Constitution fédérale stipule, dans le sens d'une mise au point, la compétence de la Confédération pour la statistique officielle. Le même article relatif à la statistique prévoit une nouvelle compétence fédérale selon laquelle la Confédération peut émettre des directives concernant les registres officiels, afin de minimiser l'effort de collecte.

Le désir des statisticiens de pouvoir effectuer des sondages de manière aussi efficace

que possible est certainement largement incontesté. Ce désir – et c'est là le motif justifiant la nouvelle compétence fédérale en matière d'harmonisation des registres – mène à solliciter que les données déjà présentes dans les registres cantonaux ne doivent pas être collectées une deuxième fois moyennant des enquêtes spéciales utilisant des formulaires. Mais comment procède-t-on pour harmoniser un registre? Relevons tout de suite l'aspect qui nous concerne essentiellement: tout d'abord on crée, pour chaque habitant, un numéro d'identification personnel (NIP), qui doit permettre de l'identifier de manière univoque à vie. Cette démarche à elle seule est déjà difficile à comprendre et constitue un comportement contradictoire de l'Office fédéral de la statistique (OFS) qui à la suite du recensement 2000 avait fait savoir que le NIP «ne s'accordait pas avec la tradition politique de notre pays» et que le changement de méthode envisagé permettrait déjà de faire des économies substantielles. Cette déclaration peut aujourd'hui encore être consultée sur Internet (cf. http://www.census.ch/chap02/fmodernisierung.html) Ce qui intrigue cependant fortement la protection des données est le fait que l'OFS continue à promouvoir l'utilisation de ce NIP pour des applications non-statistiques sous le titre «Coordination avec d'autres projets». Une telle démarche ignore tout simplement le fait que, vu sous l'angle du droit de la personnalité, ces traitements administratifs sont d'une toute autre qualité que les traitements statistiques. De plus, la discussion nécessaire de savoir si un NIP universel devait être introduit en Suisse pour des raisons administratives est ainsi tout simplement évitée. La conclusion la plus importante à tirer de cette situation est que la question du NIP doit être rayée du projet de l'OFS.

11. International

11.1. Conseil de l'Europe

11.1.1. Travaux du CJPD: protection des données et vidéosurveillance, protection des données, données policières et données judiciaires en matière pénale

Le Groupe de projet sur la protection des données (CJPD) s'est réuni du 10 au 12 octobre 2001. Il a poursuivi ses travaux dans le domaine de la vidéosurveillance et des cartes à puce.

Le CJPD a achevé la première lecture d'un projet de principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéo-surveillance (voir 8e rapport d'activités 2000/2001, p. 212). Les événements du 11 septembre 2001 survenus aux Etats-Unis ont marqué les travaux du CJPD. Cer-

tains Etats ont ainsi souhaité exclure du champ d'application des principes directeurs les activités de vidéosurveillance des autorités de police. Avec la majorité des experts présents, nous nous sommes opposés à cette approche, notamment du fait que les principes directeurs ne tendent pas à empêcher le recours à la vidéosurveillance à des fins de police. Ils veulent garantir que ces activités se font de manière à préserver l'équilibre entre besoin de sécurité et respect des droits et libertés fondamentales, notamment le droit à la vie privée.

Le CJPD a également pris connaissance d'un rapport d'expert sur la protection des données à caractère personnel concernant l'utilisation des cartes à puce et décidé d'établir des principes directeurs dans ce secteur également. Il a pris note de l'état d'avancement des travaux du groupe de travail sur la protection des données et les données policières et judiciaires en matière pénale (voir ci-dessous). Il n'est pas exclu que le CJPD procède à une révision de la Recommandation n° R (87) 15 visant à réglementer l'utilisation des données à caractère personnel dans le secteur de la police. Il a également pris connaissance de l'état d'avancement des travaux du groupe de travail sur la génétique humaine chargé d'élaborer un protocole additionnel à la Convention sur la bio-médecine et les droits de l'homme (voir ci-dessous) et réaffirmé que ce protocole devait également couvrir les secteurs des assurances et de l'emploi. Enfin, il a tenu une réunion conjointe avec le T-PD au sujet du futur des comités du Conseil de l'Europe en charge de la protection des données. A terme, les deux comités devraient fusionner et constituer un comité conventionnel élargi.

11.1.2. Travaux du T-PD: clauses contractuelles, évaluation de la Convention 108, conséquences des attentats de septembre 2001

Le Comité consultatif de la Convention 108 (T-PD) a tenu sa 17e réunion du 8 au 9 octobre 2001. Il a poursuivi ses travaux relatifs aux clauses contractuelles et son évaluation de la Convention.

Sous présidence suisse, le T-PD a poursuivi son évaluation de la Convention 108 afin de déterminer si cet instrument international, dont on a célébré le 20e anniversaire, devait être mis à jour soit par amendement, soit par l'adoption de protocoles additionnels. Cette évaluation a été au centre de la Conférence européenne sur la protection des données «Présent et avenir de la Convention 108 du Conseil de l'Europe pour la protection des données à l'égard du traitement automatisé des données à caractère personnel» qui s'est tenue à Varsovie du 19 au 20 novembre 2001 (voir http://www.legal.coe.int/dataprotection). Il ressort de cette conférence que la Convention garde toute sa pertinence et qu'il n'y a pas lieu d'envisager à ce stade une révision substantielle.

Le T-PD a décidé de ne pas procéder à la révision du «contrat type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données» qu'il avait adopté en 1992, ceci afin d'éviter des chevauchements avec les travaux entrepris dans d'autres instances internationales et notamment par la Commission des Communautés européennes. Il a par contre décidé d'élaborer des lignes directrices ou des principes directeurs à prendre en considération dans les contrats relatifs au transfert de données personnelles entre les parties à la Convention 108 et les pays tiers n'offrant pas un niveau de protection adéquat. Ces lignes directrices devraient être inclues dans un guide.

Le T-PD a procédé à un échange de vue sur la situation issue des attaques terroristes du 11 septembre 2001. Il a pris note d'une déclaration de son président dont la teneur est la suivante:

«Nous avons tous été ébranlés par les attaques terroristes ignobles qui ont endeuillé l'Amérique le 11 septembre dernier. Tout aussi inadmissible ont été l'attentat du 27 septembre contre le parlement du canton de Zoug en Suisse et celui perpétré contre le Parlement indien, le 1er octobre. Au côté des milliers de victimes innocentes et de leur famille, ces crimes abominables et monstrueux nous frappent et nous concernent tous, car ils violent les droits de l'homme et la démocratie. Ces actes, par leur brutalité et leur non sens, ont changé ou vont changer la face du monde. La criminalité et la cybercriminalité sont plus que jamais une réalité. Nous sommes tous d'accord sur la nécessité de combattre le crime et le terrorisme. Les moyens à utiliser et l'analyse des besoins diffèrent néanmoins. Un renforcement de la lutte contre le terrorisme, notamment par une amélioration des mécanismes et des moyens de coopération entre Etats et entre organisations internationales s'avérera peut-être indispensable. Ce combat légitime doit cependant se faire avec les armes de la démocratie et du droit.

Au lendemain de ces événements tragiques, plusieurs voix aux Etats-Unis et en Europe ont réclamé une remise en cause de la protection de la vie privée, accusant la protection des données de protéger les criminels et d'avoir permis ces attentats. Des mesures restrictives ont été proposées et des projets de loi sont en préparation. Or comme cela a été rappelé lors de la 23e Conférence internationale des commissaires à la protection des données «Vie privée – Droit de l'Homme» qui s'est tenue du 24 au 26 septembre à Paris, il convient de conserver une attitude prudente et responsable. Nous devons garantir un équilibre entre la sécurité des personnes et des biens et le respect des libertés individuelles, notamment de la vie privée et de la protection des données. La voie est certes étroite, mais gardons à l'esprit que des restrictions outrancières aux droits fondamentaux affecteront nos libertés de manière durable et porteront une atteinte irréversible à la démocratie, faisant en cela le jeu du terrorisme.

Plus que jamais, le Conseil de l'Europe, notamment par le biais de notre comité, se doit de jouer un rôle actif pour promouvoir et défendre le droit à la protection des données. La vie privée est un droit de l'homme. La protection des données devient un élément irréductible de la citoyenneté universelle et en tant que tel constitue un droit de l'homme. L'article 9 de la Convention 108 permet des dérogations à certaines dispositions de la convention lorsqu'elles sont prévues par la loi et constituent une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'Etat, à la sûreté intérieure et à la répression des infractions pénales. Aujourd'hui déjà les autorités de police et de lutte contre le crime organisé disposent de vastes moyens d'investigation et sont légitimés à traiter les données personnelles nécessaires à leurs actions prises en application de l'article 9. Avant d'envisager de nouvelles dérogations, il faut examiner si la survenance de ces attentats est due à un manque de moyens. Or tout porte à croire que les déficiences constatées dans l'utilisation des moyens existants et dans l'analyse des informations à disposition ne peuvent être incriminées à la protection des données. Si des mesures complémentaires apparaissent à l'avenir nécessaires, elles ne devront pas constituer un blanc seing, mais faire l'objet d'un examen sérieux, être conforme au principe de proportionnalité, répondre à un intérêt général d'une importance particulière et respecter le principe de la légalité.

Face à la globalisation des échanges et au développement planétaire des réseaux de communication, face aux risques engendrés par ces phénomènes, nous avons un rôle important à jouer dans la recherche d'un juste équilibre entre les impératifs de sécurité et la garantie du droit à la protection des données, lequel doit plus que jamais revêtir un caractère universel. Nous nous devons d'être attentifs face aux tentations de certains de prendre des mesures irréfléchies et hâtives, lesquelles pourraient entraîner un déséquilibre irréversible. Au nom de la sécurité, nous n'avons pas le droit de renoncer à des principes et des libertés fondamentales qui caractérisent les Etats de droit. Si des restrictions nouvelles devaient être introduites, elles devraient être limitées dans le temps et être accompagnées de garanties pour éviter que des citoyens innocents en soient les victimes. L'affaiblissement de la protection des données n'entraîne pas nécessairement un accroissement de la sécurité des individus. Ainsi aux termes de la présente réunion, le T-PD pourrait réaffirmer l'importance de la protection des données dans la défense de la démocratie et rappeler le rôle du T-PD. Afin de garantir l'équilibre entre le respect des droits et libertés fondamentales et la sécurité, nous pourrions de la sorte manifester notre volonté de participer de manière constructive à l'examen des mesures qui pourraient être prises pour renforcer la lutte contre le terrorisme et le crime organisé, si de telles mesures s'avèrent nécessaires».

Le T-PD a ainsi souligné que la protection des données personnelles ne rend pas impossible l'investigation et la répression des infractions pénales et la lutte contre le

terrorisme. Il convient cependant de maintenir un équilibre entre les exigences de la lutte contre le terrorisme et le respect des droits et libertés fondamentales, notamment le droit à la vie privée. Des mesures disproportionnées pourraient affecter ces droits de manière durable et irréversible. Il estime ainsi nécessaire de tenir compte de la réglementation sur la protection des données dans le cadre de l'examen des mesures normatives en matière de lutte contre le terrorisme proposées par les Ministres européens de la justice.

11.1.3. Groupe de travail du Conseil de l'Europe sur la protection des données et les données policières et judiciaires en matière pénale

Le groupe de travail sur la protection des données et les données policières et judiciaires en matière pénale (CJPD/GTPJ) a reçu de la part du groupe de projet sur la protection des données du Conseil de l'Europe (CJPD) le mandat d'examiner l'incidence des principes de protection des données sur la coopération judiciaire et policière en matière pénale.

Dans le cadre de la première partie de son mandat, le groupe de travail a entamé un examen de l'impact des principes de la protection des données sur la coopération judiciaire en matière pénale. Il a notamment élaboré des principes communs qui doivent être pris en compte lors de demandes d'assistance judiciaire de pays qui n'ont pas une protection des données adéquate.

Le groupe de travail a d'autre part entrepris en 2002 la troisième évaluation de la Recommandation N° R (87) 15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Cette nouvelle évaluation doit prendre en compte les deux évaluations précédentes ainsi que les résultats du séminaire sur la protection des données dans le secteur de la police qui s'est tenu à Strasbourg en décembre 1999. Elle ne devrait pas être restreinte aux thèmes mentionnés dans la Recommandation n° (87) 15 mais devrait étendre ses considérations aux nouveaux thèmes qui se seraient présentés depuis ainsi qu'aux nouvelles technologies policières.

11.1.4. Projet de protocole sur la génétique humaine

Les travaux d'élaboration d'un protocole sur la génétique humaine se sont poursuivis. Il a été définitivement décidé d'élargir le domaine d'application du protocole aux secteurs de l'emploi et des assurances.

Le protocole sur la génétique humaine est un protocole additionnel à la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine (Convention

d'Oviedo). Ce protocole devrait permettre d'interdire toute discrimination d'une personne en raison de son patrimoine génétique (cf. également 8e Rapport d'activités, 2000/2001, p. 215). La sixième et la septième réunions du groupe de travail ont eu lieu du 3 au 5 et du 17 au 19 avril 2001 à Strasbourg.

Au cours de ces deux réunions, le chapitre concernant le domaine de la santé a été à nouveau remanié. Le groupe de travail est parvenu à la conclusion que les analyses génétiques ne devaient être autorisées que si elles étaient accompagnées d'un conseil génétique. S'agissant d'un domaine extrêmement sensible, il convient d'informer la personne concernée de manière complète. La transparence n'est pas seulement un impératif relevant du droit de la protection des données; elle est également requise du point de vue médico-éthique. Il convient en particulier d'informer la personne concernée du but et de la nature du traitement des données, des risques possibles et des diagnostics. Il est également décisif de montrer à la personne concernée les éventuelles possibilités de conseil en rapport avec les résultats des analyses.

Jusqu'ici, le projet de protocole ne contient pas de dispositions qui prescriraient aux Etats la mise en place de commissions d'éthique dans le domaine de la génétique humaine. Ces commissions d'éthique auraient par exemple pour mission d'élaborer des critères de contrôle de la qualité des recherches et des enquêtes génétiques.

Par ailleurs, le groupe de travail a décidé d'intégrer au domaine d'application du protocole le secteur des assurances et celui de l'emploi. Il s'agit d'une initiative heureuse du point de vue de la protection des données. Le danger d'éventuelles discriminations dans ces secteurs n'est pas à négliger. L'actuel projet de protocole prévoit que les analyses génétiques sont fondamentalement interdites dans le secteur de l'emploi. Les seules exceptions possibles pourraient être justifiées par la présence de certains risques pour la santé, liés à l'emploi en question et qui ne pourraient être évités autrement.

Les prochaines réunions du groupe de travail seront l'occasion de définir si et dans quelle condition les analyses génétiques doivent être autorisées dans le secteur des assurances. Les autres chapitres du protocole sont consacrés à la sphère privée et à l'information de l'opinion publique.

11.2. Union européenne

11.2.1. Conférence européenne des commissaires à la protection des données

Les commissaires européens à la protection des données ont tenu leur Conférence de printemps à Athènes, les 10 et 11 mai 2001. Nous y avons assisté avec le statut d'observateur. La Conférence a adopté deux déclarations. La première concerne la conservation des données de trafic par les fournisseurs de services Internet. La deuxième a trait à la Charte des droits fondamentaux de l'Union européenne qui reconnaît la protection des données comme l'un des droits fondamentaux de l'Homme.

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 rang d'observateur. Cette conférence permet un échange approfondi sur les politiques de protection des données et l'évolution des législations dans les différents Etats européens. Elle débouche également sur l'élaboration de solutions communes.

La Conférence d'Athènes a abordé les thèmes du cybercrime, des télécommunications, de l'Internet, de la protection des salariés, des technologies renforçant la confidentialité des informations, du consentement, des listes noires et du commerce électronique. Le consentement préalable au traitement de données personnelles joue un rôle fondamental dans le droit européen de la protection des données. Les commissaires se sont interrogés sur la question de savoir si le consentement en tant qu'expression du droit à l'autodétermination en matière d'informations était, dans les cas où il est requis, une garantie suffisante pour légitimer le traitement de données personnelles. Le consentement ne peut pas tout légitimer et les principes de base de la protection des données, telle que la proportionnalité et la finalité peuvent limiter sa portée. Le consentement ne doit pas porter une atteinte aux éléments essentiels des droits et libertés fondamentales de l'individu et mettre en péril les droits d'autres personnes.

En relation avec le secteur des télécommunications et de l'Internet, les commissaires ont exprimé leur préoccupation à l'égard des projets selon lesquels les fournisseurs de services Internet devraient conserver les données de trafic au-delà de ce qui est requis aux fins de facturation afin de permettre l'accès éventuel à ces données par les services chargés de la mise en œuvre de la loi. La Conférence a ainsi adopté une déclaration dans laquelle elle souligne qu'«une telle conservation des données consti-

tuerait une atteinte inappropriée aux droits fondamentaux garantis à toute personne par l'article 8 de la Convention européenne des droits de l'homme et à l'égard du traitement des données, par la Convention de 1981 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel». Les commissaires réaffirment ainsi que «lorsque des données de trafic doivent être conservées dans des cas spécifiques, le besoin doit être démontré, la période de conservation doit être aussi courte que possible et la pratique doit être réglementée de manière claire par la loi».

La Conférence a également adopté une déclaration sur l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Les commissaires soulignent en particulier le fait que cette disposition de la Charte «renforce les dispositions sur la protection des données qui ont été adoptées au cours de ces quelques dernières années, de sorte que la protection des données est finalement reconnue comme l'un des droits fondamentaux de l'Homme».

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

Dans le cadre de la Conférence européenne des Commissaires à la protection des données, un groupe de travail a été créé avec pour objectif d'examiner les moyens de collaboration et de coopération entre autorités de contrôle de protection des données lors de l'examen des plaintes qu'elles traitent et des inspections ou contrôles qu'elles effectuent.

La Conférence européenne des Commissaires à la protection des données a mis en place un groupe de travail (Complaints handling Workshop) 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. La Suisse y participe également suite à l'option prise d'intégrer à ces travaux les Etats bénéficiant d'une décision de la Commission des Communautés européennes constatant un niveau de protection des données équivalent.

Le groupe de travail a pour objectif d'examiner les moyens de collaboration et de coopération entre autorités de contrôle dans le cadre de l'examen des plaintes qu'elles traitent et des inspections ou contrôles qu'elles effectuent, en tenant notamment compte de l'accroissement exponentiel des traitements de données transfrontaliers. Dans ce sens, le concept de processus de contrôle que nous avons élaboré pour nos propres tâches de surveillance a été présenté à la réunion de Lisbonne en novembre 2001. Plusieurs autorités de protection des données nationales, confrontées

aux mêmes problèmes que nous lors de la réalisation de contrôles, ont décidé de reprendre de nombreux éléments de ce concept dans leurs mécanismes de surveillance. En outre, une étude comparative sur les procédures de contrôle dans les différents Etats a été initialisée sur la base de notre concept de contrôle. Les travaux sur les étapes et les processus de contrôle seront poursuivis lors de la prochaine réunion prévue à Dublin en 2002.

Afin de faciliter les échanges d'informations entre ses membres, le groupe de travail utilise le système informatique CIRCA (Communication & Information Resource Centre Administrator). Il s'agit d'un système extranet sécurisé lié au programme IDA (Interexchange of Data between Administrations) de la Commission européenne et offrant un accès restreint avec mot de passe. Il a pour but de favoriser les échanges d'informations sur les plaintes transnationales, la communication des résultats des contrôles effectués ainsi que les échanges d'expériences nationales pouvant intéresser les autres autorités de protection des données. Lors de la réunion de Lisbonne, de nombreux intervenants ont 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 aussi à des Etats tels que la Suisse ayant un niveau de protection équivalent.

11.3. OCDE

11.3.1. Groupe de travail sur la sécurité de l'information et la protection de la sphère privée (WISP)

Au cours de l'année écoulée, le groupe de travail a concentré ses activités sur les mécanismes de règlement des litiges en cas de transactions en ligne, les technologies respectueuses de la protection des données, la génétique humaine, les règles de comportement dans le domaine du commerce électronique et, enfin, sur les répercussions des événements du 11 septembre 2001.

Divers modèles de règlement extrajudiciaire des litiges en cas de transactions en ligne ont été présentés au groupe de travail et analysés. Il convient au préalable d'examiner les questions de droit en relation avec les transactions transfrontalières afin de déterminer quel est le droit applicable en cas de litige. La difficulté de la tâche est accrue par le fait que quelques Etats membres cherchent à utiliser ces mécanismes de règlement des litiges pour exclure la voie judiciaire normale. Pour cette raison, un inventaire de tous les mécanismes de règlement des litiges en cas de transactions en ligne

sera établi dans un premier temps. Dans une seconde phase, l'applicabilité des différents modèles sera examinée.

A propos de la protection de la sphère privée sur Internet, le groupe de travail a souligné l'importance des technologies respectant la protection des données (Privacy Enhancing Technologies, PET). Différentes méthodes techniques allant dans ce sens ont été présentées au cours d'une rencontre spécialement consacrée à ce thème. De plus en plus d'entreprises prennent aujourd'hui conscience que la protection de la sphère privée est un facteur important grâce auquel elles peuvent gagner la confiance des consommateurs dans le domaine du commerce électronique. Elles sont toujours plus nombreuses à mettre au point des méthodes techniques garantissant la protection de la sphère privée et les mettent gratuitement à la disposition des utilisateurs. Ces technologies ont été présentées au groupe de travail, ainsi que leurs principaux avantages pour les consommateurs et les utilisateurs d'Internet. Par ailleurs, le groupe de travail a reconnu que ces technologies à elles seules ne suffisaient pas à protéger la sphère privée. D'une part, elles ne peuvent pas remplacer la protection juridique, de l'autre elles sont trop peu connues du grand public.

La plupart de ces technologies ne comportant aucune information sur leur fabricant ou sur leur fonctionnalité, les utilisateurs sont tenus de s'y fier aveuglément. Le groupe de travail déplore également que les différents besoins des utilisateurs d'Internet en matière de sécurité ne soient pas suffisamment pris en compte par les fabricants. Il a demandé que ces éléments soient considérés lors de la mise au point de ces technologies et que l'on tienne davantage compte des divers besoins des utilisateurs.

Par ailleurs, le groupe de travail entend chercher des solutions qui permettent d'attirer l'attention des consommateurs et des utilisateurs d'Internet sur les technologies garantissant leur sphère privée. Il élabore à cet effet un document d'information sur l'utilisation judicieuse de ces technologies dans le but de protéger la sphère privée.

Le groupe de travail s'est également penché sur la génétique humaine. Il a souligné que les informations génétiques sont des données beaucoup plus sensibles que les données médicales, qu'elles ne peuvent donc pas être classées dans la même catégorie et doivent faire l'objet d'un traitement et d'une protection spécifiques. Le fait que l'obtention de données génétiques puisse avoir des conséquences non seulement pour la personne concernée, mais aussi pour toute sa famille a été particulièrement relevé. Un comité ad hoc est chargé d'élaborer une étude résumant les différents problèmes pouvant surgir lors du traitement de données génétiques compte tenu des travaux déjà effectués par le Conseil de l'Europe. Cette étude permettra de planifier de manière judicieuse les tâches futures du groupe de travail.

Pour ce qui est des travaux relatifs aux règles de comportement dans le commerce électronique, nous avons à nouveau relevé que ce genre de règles ne constitue pas une solution de rechange aux dispositions légales. Le groupe de travail a reconnu néanmoins que les règles de comportement peuvent donner une plus grande transparence à l'application des obligations légales. Un inventaire des différents modèles sera établi afin de pouvoir analyser l'efficacité de ces règles. Il permettra de déterminer quelles règles de comportement répondent aux principes de l'OCDE afin d'analyser l'efficacité des mécanismes d'application et de déterminer les conditions nécessaires à l'établissement de ces règles. Nous avons informé le groupe de travail que le PFPD a déjà pris position sur les règles de comportement et sur la sphère privée dans le commerce électronique (cf. http://www.edsb.ch/f/themen/e-commerce/index.htm).

Le groupe de travail s'est également penché sur les conséquences des événements du 11 septembre 2001. Il estime à l'unanimité que malgré ces attentats terroristes, les buts et travaux du groupe de travail doivent rester placés sous le signe du pragmatisme et de l'objectivité. C'est la raison pour laquelle le groupe de travail concentre ses activités sur le remaniement de la directive relative à la sécurité des données; en effet, la situation en matière de sécurité a subi des bouleversements radicaux depuis l'adoption des directives en 1992. Les principes neutres du point de vue technologique seront conservés, mais adaptés au contexte actuel des systèmes globaux et mis en réseaux au niveau mondial.

11.4. Autres thèmes

11.4.1. Conférence internationale des commissaires à la protection des données

La XXIIIe Conférence internationale des commissaires à la protection des données s'est déroulée à Paris du 24 au 26 septembre 2001. Intitulée «Vie privée – Droit de l'homme», elle réunissait des délégations provenant de près de 50 Etats et des cinq continents. La Conférence a réaffirmé le caractère universel du droit à la protection des données. Les commissaires à la protection des données ont adopté une nouvelle procédure d'accréditation des autorités de protection des données personnelles et de la vie privée habilitées à participer à la conférence internationale.

La XXIIIe Conférence internationale des commissaires à la protection des données s'est déroulée dans le cadre de la Sorbonne à Paris. Plus que jamais, l'Homme en tant

que citoyen, salarié, patient, consommateur, internaute ou individu était au centre des débats. La Conférence s'est en effet voulu un large forum des droits et des libertés. Bien que les événements tragiques du 11 septembre 2001 aient fortement marqué les esprits des participants et influencés les discussions, la Conférence a clairement rappelé que «la vie privée est un droit de l'homme. La protection des données devient un élément irréductible de la citoyenneté et en tant que tel constitue un droit de l'homme». Face à la globalisation et à la dimension planétaire des traitements de données personnelles, ce droit fondamental à la protection des données doit tendre à un caractère universel par la recherche de règles communes. La sécurité des personnes et des biens et notamment la lutte contre le terrorisme sont légitimes et non contestées. Cela ne doit pas cependant déboucher sur des mesures inconsidérées qui rendraient illusoires les droits et les libertés individuelles. Il n'est pas nécessaire d'affaiblir le respect du droit à la vie privée pour obtenir plus de sécurité. Au contraire, l'application stricte des législations de protection des données peut offrir plus de sécurité. Les circonstances actuelles imposent «collectivement, d'être plus attentifs, sinon plus vigilants, à certains déplacements de curseur entre sécurité et liberté qui seraient irréfléchis ou précipités» et qui remettraient en cause de manière irrémédiable les fondements de nos démocraties. Il est impératif de maintenir un juste équilibre entre besoin de sécurité et respect des libertés individuelles.

Alternant séances plénières et ateliers, la Conférence a permis de faire le point sur l'évolution du recours aux technologies de l'information en général et de manière sectorielle. Elle a permis aux commissaires d'être à l'écoute des préoccupations de nombreux acteurs de la société de l'information. Elle a permis d'identifier de nouveaux risques liés en particulier à la vidéosurveillance avec reconnaissance des visages, à la cybersurveillance, aux techniques de localisation ou à la biométrie. Elle a rappelé que les technologies sont également une chance pour protéger la vie privée. Dans cette optique, les commissaires ont un rôle actif à jouer dans la formation, la sensibilisation et la promotion de ces technologies et des outils de protection, dont ils doivent accompagner le développement. Cela implique que les concepteurs intègrent suffisamment tôt les exigences de la protection des données et consultent les autorités compétentes.

Lors d'une séance plénière «Vie privée, vie salariée», nous avons eu l'occasion de présenter le résultat de nos investigations relatives aux tests de dépistage de la drogue sur le lieu de travail. A cette occasion, nous avons rappelé que:

- Les tests de dépistage de drogues pratiqués par de nombreuses entreprises auprès de leurs employés ou de certaines catégories d'employés constituent:
- une atteinte à la vie privée de l'individu;

- une infraction au droit du travail;
- une non-considération de la politique actuelle en matière de drogue; en outre,
- la fiabilité des résultats n'est pas démontrée. Ils ne mesurent pas le niveau d'altération des facultés découlant de l'usage de drogues et par conséquent ne peuvent pas être utilisés pour évaluer la capacité d'une personne à exécuter un travail.
- Il convient de privilégier l'information et la formation afin de responsabiliser les travailleurs qui occupent des postes critiques pour la sécurité.
- Il convient de mettre en place des programmes d'accompagnement et de sensibilisation permettant d'atteindre des résultats positifs, sans passer par des tests de dépistage.
- Des tests de dépistage ne peuvent être tolérés que s'il existe un risque majeur pour la sécurité des personnes, des biens ou de l'environnement, pour autant que les autres moyens de prévention des risques soient insuffisants et qu'il n'y ait pas d'autres moyens moins attentatoires à la vie privée de s'assurer que le travailleur ne présente pas un risque pour la sécurité (notamment supervision).
- Des tests de dépistage ne peuvent pas se justifier pour des postes non critiques pour la sécurité.
- Ces tests doivent être effectués de manière à protéger la confidentialité et à respecter le secret médical. En l'absence de dispositions légales, le consentement libre, informé, spécifique et explicite des personnes concernées doit être requis.
- Ces tests ne peuvent reposer sur le seul consentement des personnes concernées. Il serait souhaitable que le législateur fixe le cadre de tels tests et que toutes les catégories d'employés occupés à un travail présentant un risque majeur pour la sécurité soient touchées.
- Le législateur devrait préciser quels types de substances sont constitutives d'un risque élevé, définir les métiers où l'affaiblissement des facultés lié à la consommation de drogues peut représenter un grave danger et également dresser la liste des drogues qui causent des effets connus d'affaiblissement des facultés à court ou à long terme.

Enfin lors de la séance réservée aux seuls commissaires à la protection des données, ceux-ci ont adopté une nouvelle procédure d'accréditation des autorités de protection des données personnelles à la conférence internationale (voir annexe, page 127). Les documents de la Conférence sont accessibles à l'adresse http://www.paris-confe-

rence-2001.org .

11.4.2. 30e séance du Groupe de travail international pour la protection des données dans le domaine des télécommunications

Le PFPD a participé, du 27 au 30 août 2001 à Berlin, à la réunion d'automne du groupe de travail qui se réunit deux fois par an. En plus de l'échange des derniers développements au niveau national dans le domaine du droit sur les télécommunications ainsi que dans le domaine de l'Internet, la discussion a surtout porté sur les sujets suivants: vote électronique, profilage en ligne et surveillance des activités Internet à la place de travail.

Fidèle à la tradition, le préposé berlinois à la protection des données et à la liberté d'information a organisé dans le cadre du salon «Internationale Funkaustellung» un symposium public sur le thème «Protection des données et propriété intellectuelle sur Internet». Vous trouverez des informations plus détaillées sur Internet à l'adresse

http://www.datenschutz-berlin.de/doc/int/iwgdpt/index.htm ou

http://www.datenschutz-berlin.de/infomat/heft29/index.htm.

12. Le Préposé fédéral à la protection des données

12.1. Huitième Conférence suisse des Commissaires à la protection des données

La huitième Conférence suisse des Commissaires à la protection des données, organisée par le préposé cantonal bernois à la protection des données, s'est tenue à Berne le 22 novembre 2001. Elle a réuni les représentants des autorités cantonales en charge de la protection des données et les conseillers à la protection des données des départements fédéraux.

Les participants à la conférence ont abordé la question de la sécurité intérieure telle qu'elle se présente depuis les événements du 11 septembre 2001 et ont relevé que la sphère privée des citoyens était de plus en plus menacée par l'élargissement des tâches publiques. En effet, plus l'Etat étend son domaine d'action, plus la masse des informations traitées augmente. Afin d'éviter les abus dans l'accomplissement de ces nouvelles tâches, nous avons demandé que les mécanismes de contrôle en matière de protection des données soient renforcés, parallèlement à une intensification des activités dans le domaine de la sécurité intérieure.

L'essentiel des discussions a néanmoins porté sur la place des préposés à la protection des données au sein des projets informatiques. Les responsables de projet et les spécialistes de la sécurité ont souligné l'importance extrême de l'intégration précoce des préposés à la protection des données aux projets informatiques. Cette intégration permettra de déceler à temps les dangers menaçant les droits de la personnalité des personnes concernées, de définir de manière proportionnée les droits d'accès, de garantir la sécurité des données et de diminuer les coûts. Les intervenants ont en outre relevé qu'aujourd'hui, dans la plupart des cas, les projets informatiques sont élaborés sans prescription de protection des données et, de ce fait, sont difficilement contrôlables. Les autorités de protection des données ont requis une participation plus grande lors de la mise au point de ce genre de projets, ce qui supposerait de plus larges ressources informatiques pour les services de surveillance.

12.2. Les publications du PFPD – Nouvelles parutions

- Bulletin d'information du PFPD 2/2001
- Bulletin d'information du PFPD 1/2002

Le nouveau site du PFPD

Nous avons procédé à un remaniement fondamental de notre offre sur Internet au 1er février 2002. Les textes se rapportant à des thèmes particuliers sont désormais regroupés en un seul endroit et un glossaire a été constitué pour faciliter les recherches sur des questions spécifiques. En outre, notre site offre la possibilité de s'inscrire sur une liste pour être régulièrement informé des nouvelles parutions du PFPD. (www.edsb.ch)

Autres informations sur les thèmes suivants:

- La Poste et la loi sur le blanchiment d'argent – pourquoi la Poste a le droit de photocopier les documents d'identité (www.edsb.ch/f/themen/weitere/post-gwg.htm)
- Protection des données lors de recherches généalogiques (www.edsb.ch/f/themen/weitere/genealogie.htm)
- Appréciation du système de rémunération des pharmaciens basée sur les prestations (RBP) (www.edsb.ch/f/themen/gesundheit/loa.htm)

12.3. Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2001 au 31 mars 2002

Participations à des conférences:

Nationales	Internationales
13	23

Nombre de séances

	Confédération	Personnes privées	Cantons
A l'intérieur	119	80	11
A l'extérieur	151	44	29
Total	**270**	**124**	**40**

Nombre de prises de position

	Entrées	Prises de position écrites	Recommanda-tions du PFPD	Pas d'objections
Sur des lois	55	51		8
Sur des ordonnances	63	60		5
Sur des traités internationaux	34	32		4
Questions du secteur public:				
Organes fédéraux	283	187	1	5
Cantons	60	33		
Autorités étrangères de protection des données	28	26		
Questions du secteur privé:				
Personnes privées	202	172	1	9
Banques	27	26	1	
Vente d'adresses / Marketing direct	64	35		
Crédit	33	33		
Librairies/Publications	10	10		
Secteur du TED	27	23		
Personnel	256	224		
Télécommunication	39	39		
Assurances	55	47		
Affaires de police	106	106		
Santé	132	106		
Droit de bail	8	7		
Carte client	8	3		
Sectes	6	3		
Environnement / constructions	1	1		
Associations	21	21		
Impôts	6	6		
Statistiques et recherche	2	2		
Total	**1526**	**1253**	**3**	**31**

RENSEIGNEMENTS PAR TELEPHONE	Personnes privées	Organes fédéraux	Cantons	Associations / Fédérations	Secteur du TED	Avocats / Fiduciaires	Industrie / Entreprises de Services	Médias
Protection des données en général	243	59	52	15	16	119	159	40
Droit d'accès	120	27	1	6		2		11
Annonce de fichiers	37	13				88	56	
Communication de données	58	10	5	54	18	39	94	42
Flux à l'étranger	68	11		10	39	103	72	9
Compatibilité avec les pays de l'UE	85	8	2		14	56	40	12
Secteur du travail/ Placement	178	11	2		32	59	97	39
Santé/Assurances	177	54	22	7	14	49	31	33
Droit de bail Formulaires	18							
Marketing direct/Publicité	28			11		28	32	34
Banques/ Crédits Renseignements	65	1		8	2	32	10	9
Poste	16	2		6	4	1		
Recherche	3	1		1		1		1
Statistiques	29	29	6					38
Surveillance vidéo	52	3		1	9		2	37
Téléphone IRNS/ Données Télécom	31	4		8		3	28	27
INTERNET	75	5	2	5	6	7	12	43
Sécurité des données/Cryptographie	22	15	1		23	8	9	20
Affaires de police	36	39	5					21
Asile / Étrangers	9	18	1			2		
Total	**1352**	**317**	**101**	**132**	**177**	**597**	**642**	**416**

12.4 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:	Eggli Liliane, lic. phil. Tsiraktsopulos Kosmas, lic. en droit
Service juridique:	8 Personnes
Service informatique:	5 Personnes
Chancellerie:	3 Personnes

13. Annexes

13.1. Règlement-type régissant la surveillance du courrier électronique et de l'utilisation d'Internet sur le lieu de travail

Règlement type relatif à la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail

Le texte du règlement est écrit en caractères droits; les notes et les commentaires sont en italiques.

Vous trouverez de plus amples explications dans le «Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail» (Guide), qui peut être obtenu au secrétariat du PFPD.

1. Remarques générales

1.1 Intérêts de l'employeur

L'utilisation, sur le lieu de travail, d'un ordinateur connecté à un réseau peut porter atteinte à certains intérêts et à certains équipements techniques de l'employeur. Peuvent être affectés:

- la capacité de la mémoire de stockage et la bande passante du réseau, par suite d'une utilisation excessive d'Internet et du courrier électronique;
- la sécurité des données et des applications (disponibilité, intégrité, confidentialité) par l'importation de virus, de vers, de chevaux de Troie ou par l'installation de logiciels étrangers à l'entreprise);
- le temps de travail et d'autres intérêts financiers (pertes de productivité, augmentations de coûts liées aux moyens et/ou prestations supplémentaires, frais de réseau, etc.);
- d'autres intérêts de l'employeur protégés par la loi tels que sa réputation, ses secrets de fabrication et d'entreprise ou la protection des données.

1.2 Intérêts de l'employé

Notre entreprise respecte et protège la personnalité de l'employé; elle porte une attention particulière à sa santé et s'attache à préserver la moralité.

Elle ne traite de données relatives aux employés que dans la mesure où elles concernent son aptitude à remplir les tâches inhérentes au contrat qui le lie à son employeur ou sont nécessaires à l'exécution de ce contrat; elle informe l'employé lorsqu'elle traite ou entend traiter de telles données.

Notre entreprise n'utilise aucun système de contrôle destiné à surveiller le comportement des employés sur le lieu de travail. Si le recours à de tels systèmes s'impose pour d'autres fins, ils sont choisis ou conçus de telle façon qu'ils ne portent atteinte ni à la santé, ni à la liberté de mouvement des employés.

2. Règlement d'utilisation

2.1 Autorisation d'utiliser Internet et le courrier électronique sur le lieu de travail

Les catégories d'employés ci-après ont accès à Internet et/ou sont autorisées à utiliser le courrier électronique:

- …
- …
- …

Indiquer les catégories d'employés ainsi que le but de l'utilisation, cette dernière devant être définie en fonction des besoins professionnels effectifs de la catégorie considérée.

2.2 Etendue de l'utilisation d'Internet et du courrier électronique sur le lieu de travail

Il appartient au premier chef à l'employeur de déterminer si les employés sont autorisés ou non à utiliser Internet et le courrier électronique à des fins privées sur le lieu de travail. Comme dans d'autres domaines des rapports de travail, l'employeur a le pouvoir de donner des instructions. L'étendue de l'utilisation d'Internet et du courrier électronique peut varier selon la catégorie d'employés. L'entreprise pourra soit autoriser, soit interdire ou limiter l'utilisation des applications réseau à des fins privées. Vous trouverez au chapitre 5 de notre Guide quelques indications concernant la façon de réglementer cette utilisation.

Le présent chapitre du règlement doit fixer des règles claires et sans équivoque.

3. Règles de surveillance

3.1 Privilégier les mesures de protection techniques

Notre entreprise s'engage à prévenir d'abord par des mesures techniques les abus et les dommages techniques.

Elle actualise régulièrement ces mesures en fonction des évolutions technologiques et les adapte après chaque incident.

Elle s'engage à informer les employés des dangers que présente l'utilisation d'un ordinateur connecté à un réseau.

Elle ne peut analyser les traces laissées par les connexions Internet ou par les messages électroniques de l'utilisateur que lorsque les mesures techniques ne permettent pas d'empêcher un abus (cf. § 3.5.1 à 3.5.6).

3.2 Mesures de protection techniques

Notre entreprise met en œuvre les mesures de protection techniques suivantes:

- …
- …
- …

Les mesures de protection techniques peuvent réduire les risques liés à l'utilisation d'Internet et du courrier électronique. On privilégiera ces mesures, à caractère préventif, aux moyens répressifs tels que la surveillance de personnes. Les mesures de protection techniques les plus importantes sont notamment les sauvegardes de données (backup), les logiciels antivirus, les gestionnaires de quotas disque, les systèmes pare-feu (firewall) avec listes de sites autorisés et de sites interdits et système de détection des intrusions, le cryptage des données sensibles, la mise en veille de l'écran (screensaver) après un délai raisonnable et avec une protection par mot de passe, l'emploi de mots de passe non triviaux et intransmissibles et, enfin, la réglementation de la suppléance et de la transmission du courrier électronique. En outre, les logiciels de navigation et de messagerie doivent être adaptés aux derniers développements technologiques et être configurés de manière à assurer une sécurité optimale. Vous trouverez une liste des principales mesures de protection techniques au chapitre 3 de notre Guide.

3.3 Journalisation

La journalisation se définit comme l'enregistrement continu des données d'utilisation de type «qui, quoi, quand». Dans notre entreprise, elle est assurée aux endroits suivants:

Ici, l'entreprise doit indiquer les formes de journalisation auxquelles elle recourt, leur but et la durée de conservation des données. Le chapitre 4 du Guide présente les principaux modes de journalisation. Selon la forme de journalisation que l'entreprise entend utiliser et compte tenu des caractéristiques propres à chacune, il faut apporter, dans le règlement sur la surveillance, les précisions suivantes:

- Au niveau des **éléments de connexion interréseaux**, on procède à une journalisation de l'adresse IP («qui»), de la date et de l'heure («quand»), et de l'URL appelée («quoi»). Bien que l'URL (adresse Internet) soit une donnée d'utilisation, il est généralement possible de reconstituer le contenu après coup.
- Dans l'accès aux **services Intranet**, sont enregistrés le nom de l'utilisateur (USERID, «qui») et l'adresse IP (*lorsque celle-ci a été attribuée de manière dynamique)*. L'indication de la date et de l'heure («quand») est également enregistrée, de même que l'opération effectuée («quoi»), c'est-à-dire le fait de se connecter au système ou de s'en déconnecter, l'impression, le lancement d'une application, etc.
- Les serveurs de messagerie (interface Intranet/Internet) enregistrent les adresses de l'expéditeur et des destinataires, l'objet des messages électroniques ainsi que la date et l'heure à laquelle un message a été expédié ou lu.
- Le navigateur Web utilisé (browser) permet d'enregistrer sur le disque dur de l'ordinateur tous les accès à Internet qui ont eu lieu pendant une période donnée (*indiquer pendant combien de temps)* (historique). Ce navigateur crée aussi des fichiers temporaires (fichiers cache) et des fichiers témoins permanents (cookies) indiquant les pages Web visitées.
- *etc. (cf. chap. 4 du Guide).*

3.4 Non-utilisation de programmes espions

Notre entreprise s'abstient d'utiliser des programmes permettant d'enregistrer systématiquement et en permanence toutes les activités effectuées sur un ordinateur connecté au réseau.

3.5 Conditions générales de la surveillance

3.5.1 Confidentialité des fichiers journaux et protection du contenu des messages électroniques privés

Si le nom de l'utilisateur figure dans les fichiers journaux, ce qui est le cas avec un proxy-serveur, nous recommandons de remplacer le nom de l'utilisateur par un pseudonyme.

Comme la journalisation de l'utilisation du courrier électronique porte sur les éléments de l'adressage (adresses de l'expéditeur et du destinataire en particulier), elle référence forcément des noms de personnes. Cependant, notre entreprise ne consulte pas le contenu des messages électroniques privés. Elle recommande aux employés d'utiliser un service de messagerie distinct, si possible crypté, pour ce type de courrier afin d'en préserver la confidentialité.

La possibilité d'utiliser un service de messagerie Internet privé dépend du règlement d'utilisation. Les employés ne peuvent pas utiliser ce service si le règlement interdit l'usage d'Internet à des fins privées.

Les services informatiques de notre entreprise sont tenus de respecter la confidentialité des fichiers journaux et de la liste de correspondance susmentionnée.

3.5.2 Analyse des fichiers journaux

Est considéré comme abus toute violation du règlement d'utilisation (§ 2.2).

Nos services informatiques procèdent à l'identification du collaborateur fautif lorsque son nom d'utilisateur (ou son pseudonyme) figure dans le fichier journal ou alors à l'identification du poste de travail d'où l'abus a été commis à partir de l'adresse IP contenue dans le fichier journal. Dans ce dernier cas, l'identification de l'abuseur nécessite des investigations plus poussées, si le poste de travail est partagé par plusieurs collaborateurs.

Nous recommandons à l'entreprise de désigner une seule personne responsable du dépouillement des fichiers journaux à des fins d'identification.

Ils transmettent ensuite le résultat de leurs analyses au supérieur du collaborateur fautif, qui le sanctionnera.

Lorsque les éléments d'adressage ne permettent pas de déterminer si le message électronique est de nature privée ou de nature professionnelle, la situation doit être clarifiée avec l'employé concerné.

Les données personnelles sont traitées confidentiellement autant par la direction que par les services informatiques.

Lorsque l'abus n'entraîne pas de dérangement technique, le supérieur décide, avec les services informatiques et en fonction de la gravité de l'abus, si le dépouillement des fichiers journaux à des fins d'identification doit avoir lieu immédiatement ou uniquement en cas de récidive. Dans ce dernier cas, le supérieur informe ses collaborateurs qu'un abus a été constaté et qu'une analyse des fichiers journaux serait opérée à des fins d'identification s'il devait se renouveler.

3.6 Types de surveillance

3.6.1 Contrôle de la sécurité technique et du bon fonctionnement du système

Nos services informatiques sont chargés de garantir la sécurité technique et le bon fonctionnement du système. La sécurité est assurée par la mise en œuvre de mesures de protection techniques.

Si un dérangement survient malgré les mesures de protection techniques, les fichiers journaux peuvent être analysés afin d'établir la cause de la panne.

Les services informatiques adaptent ces mesures et informent la direction lorsque le règlement d'utilisation doit être revu.

Si le dérangement technique est dû à une utilisation non autorisée d'Internet ou du courrier électronique, les règles fixées au § 3.5.2 s'appliquent.

3.6.2 Contrôle du respect du règlement d'utilisation

L'employeur peut, s'il le souhaite, effectuer des contrôles afin de s'assurer que le règlement d'utilisation est respecté. En pareil cas, il fixera les règles de surveillance suivantes:

Nos services informatiques sont autorisés à vérifier que l'interdiction *(ou la limitation)* de l'utilisation d'Internet et du courrier électronique à des fins privées est respectée.

Les contrôles sont effectués de manière aléatoire. Ils sont anonymes et ne couvrent qu'une période d'utilisation limitée.

L'entreprise doit indiquer ici combien de jours par mois dureront ces contrôles. Notons qu'un contrôle effectué sur toute la période séparant deux sondages équivaut à une surveillance permanente du comportement du personnel et est donc interdit.

Si ces contrôles révèlent un abus, les règles fixées au § 3.5.2 s'appliquent.

3.6.3 Procédure suivie en cas de soupçon de délit

Si notre entreprise dispose d'éléments concrets donnant lieu de soupçonner qu'un délit a été commis dans l'utilisation d'Internet ou du courrier électronique, elle peut sauvegarder les preuves pertinentes, c'est-à-dire les fichiers journaux et, éventuellement, les sauvegardes (backups).

C'est le supérieur hiérarchique et non le service informatique qui décide si une plainte sera déposée ou non.

Bien qu'il n'existe aucune obligation de porter plainte, le dépôt d'une plainte est recommandé, du moins pour les délits poursuivis d'office, afin de prévenir tout risque de complicité.

Lorsque l'abus constaté a causé un dérangement technique, notre entreprise peut, si elle soupçonne l'existence d'un délit, élucider elle-même l'identité de la personne concernée. Dans les autres cas, elle portera plainte contre inconnu et ce sont les autorités chargées de la poursuite pénale qui se chargeront de l'analyse des fichiers journaux.

Notre entreprise s'engage à traiter confidentiellement le résultat des enquêtes, en particulier à ne pas le divulguer aux autres employés.

L'application de sanctions disciplinaires pour violation du règlement d'utilisation est réservée (cf. § 2.2).

3.6.4 Surveillance des prestations

On peut concevoir qu'une surveillance des prestations ait lieu dans certaines entreprises. Elle pourra être réglée comme suit:

La surveillance des prestations consiste à procéder au recensement systématique de la qualité et/ou de la quantité produite.

Dans notre entreprise, la surveillance des prestations n'a lieu que sur une durée limitée (*indiquer pendant combien de temps).*

Si un abus est constaté lors de cette surveillance, les règles fixées au § 3.5.2 s'appliquent.

3.6.5 Contrôle des affaires

Notre entreprise peut, dans le cadre du contrôle des affaires, consulter les messages professionnels reçus par courrier électronique, tels que les demandes émanant de clients. A ce titre, elle est autorisée également à ouvrir la boîte à lettre électronique des employés absents

Si aucune indication ne permet de distinguer les messages privés des messages professionnels et que les éléments d'adressage ne permettent pas de déterminer si le message est de nature privée ou non, notre entreprise peut partir du principe - comme elle le ferait pour le courrier postal - que le message est de nature professionnelle. Lorsqu'elle a de sérieuses raisons de douter du caractère professionnel du message, elle doit prendre contact avec le collaborateur afin de clarifier la situation. En pareil cas, elle n'est pas autorisée à consulter le contenu du message considéré.

(Que l'utilisation du courrier électronique à des fins privées soit autorisée ou non.)

Les mêmes règles s'appliquent lorsqu'une boîte à lettres électronique est partagée par plusieurs employés.

Si une violation du règlement d'utilisation est constatée dans le cadre du contrôle des affaires, les règles fixées au § 3.5.2 s'appliquent.

4. Sanctions en cas d'abus

Si les conditions et règles régissant la surveillance ont été respectées, notre entreprise peut, lorsqu'elle constate un abus, prendre des sanctions disciplinaires contre l'employé fautif.

L'entreprise doit énumérer ici les sanctions qu'elle compte prendre en cas d'abus. La sanction peut consister à adresser un avertissement, à bloquer l'accès à Internet, à exiger des dommages et intérêts, à supprimer une prime spéciale, etc. (cf. chap. 11 du Guide). Dans les cas extrêmes, par exemple si l'abus se reproduit malgré un avertissement et provoque une panne technique ou si le délit est établi, l'employeur peut même congédier l'employé. Le contrat de travail ne peut être résilié avec effet immédiat que si les circonstances ne permettent pas, selon les règles de la bonne foi, d'exiger de l'employeur qu'il maintienne les rapports de travail. Les sanctions doivent être adaptées à la gravité de l'abus et leur ampleur doit être définie dans le règlement relatif à la surveillance.

Le supérieur hiérarchique est compétent pour prononcer des sanctions contre l'employé fautif.

L'adresse IP, et donc en règle générale l'identité de l'employé fautif, peuvent être dissimulées délibérément. Notre entreprise s'engage à ne prendre de sanctions disciplinaires que si l'identité de l'employé fautif a pu être établie avec certitude.

On peut réduire fortement le risque de dissimulation de l'identité en utilisant un écran de mise en veille qui sera activé dans un délai raisonnable et protégé par un mot de passe.

Avant d'effacer des fichiers acquis abusivement, l'entreprise informera les employés concernés et ils pourront - pour autant que cela soit possible techniquement - transférer sur des supports de données privés les fichiers tels que les messages électroniques privés.

5. Droits de l'employé en cas de surveillance non autorisée

Si les conditions et règles régissant la surveillance de l'utilisation d'Internet et du courrier électronique ne sont pas respectées, l'employé peut faire valoir les droits prévus par le code civil en cas d'atteinte à la personnalité (cf. art. 28 ss CC).

Si l'entreprise exerce une surveillance abusive, l'employé concerné peut engager contre elle une poursuite pénale, par exemple pour violation du domaine secret ou du domaine privé au moyen d'un appareil de prise de vues (art. 179^{quater} CP) ou pour soustraction de données personnelles (art. 179^{novies} CP).

Sont aussi considérées comme surveillance abusive l'analyse des fichiers journaux sans qu'un abus ait été constaté, la consultation du contenu du courrier électronique privé et l'utilisation de programmes espions.

6. Autres dispositions

Autant les services informatiques que les responsables hiérarchiques de notre entreprise doivent protéger par des mesures techniques appropriées les données personnelles qu'ils recueillent dans le cadre d'une surveillance. Ils veillent en particulier à assurer la confidentialité, la disponibilité et l'intégrité de ces données.

L'employé peut en tout temps demander à l'entreprise si des données le concernant ont été traitées.

Les données personnelles ne peuvent être communiquées à des tiers non autorisés sans le consentement de la personne concernée ou en l'absence de motif valable. Les collègues de travail sont considérés comme des tiers au regard de la législation sur la protection des données.

L'entreprise n'a aucune obligation légale de conserver les fichiers journaux. Ces derniers peuvent être conservés pendant une durée limitée, ne dépassant généralement pas quatre semaines, dans le but de fournir des moyens de preuve.

La durée de conservation dépend du but de la journalisation. Dans le cadre des procédures de sanction ou des poursuites pénales, ils peuvent être conservés jusqu'à l'expiration du délai de recours.

13.2. Aide-mémoire relatif au thème «Rapport de sortie et d'opération»

DSB-CPD.CH

Die schweizerischen Datenschutzbeauftragten

Les Commissaires suisses à la protection des données

Notice
Lettres de sorties et rapports opératoires

De quoi s'agit-il ?

De manière à évaluer l'étendue des prestations qu'ils seront amenés à exécuter, la plupart des assureurs exigent les lettres de sortie et les rapports opératoires de la part des hôpitaux et des homes qui font partie du secteur obligatoire.

Le **lettre de sortie** synthétise le cas d'un patient ou d'une patiente à l'occasion d'un séjour dans un hôpital ou dans un home. Elle comprend en principe l'ensemble des diagnostics qui ont été faits durant ce séjour. Les diagnostics actifs sont étayés par d'autres éléments du dossier dont les conclusions sont citées. La lettre de sortie contient aussi des commentaires, ou une discussion si nécessaire, et le traitement à suivre après le départ de l'hôpital. Enfin, la lettre de sortie donne des recommandations pour le suivi médical.

Le but premier d'une lettre de sortie est par conséquent d'informer le médecin traitant qui suivra le patient ou la patiente après sa sortie.

Le **rapport opératoire** consiste à décrire le déroulement de l'opération, soit d'indiquer combien de temps la personne est restée sous anesthésie, quelle quantité de sang a dû lui être transfusée, quels gestes techniques ont été effectués par le chirurgien et d'autres personnes impliquées dans le processus.

Les lettres de sortie et les rapports opératoires sont par conséquent susceptibles de contenir des informations relatives aux patients et aux patientes, données qui sont sensibles au sens de la protection des données.

Le traitement de ces données sensibles est soumis de par les dispositions légales à des exigences accrues.

On inclut aussi dans le traitement de ces données leur communication à des tiers et leur acquisition par des tiers; dans le cas présent, la communication des lettres de sortie et des rapports opératoires aux assureurs, respectivement le traitement de ces documents par les assureurs s'y trouvent également compris.

La communication de ces données ne peut se faire que moyennant le respect des principes généraux qui guident la protection des données, parmi lesquels figurent la légalité, la conformité au but indiqué ou finalité, la nécessité ou proportionnalité et l'exactitude des données transmises.

But de la collecte des données par les assureurs

La collecte par les assureurs des données relatives aux assurés a pour but de déterminer s'ils doivent payer les soins et de permettre en particulier de fixer l'étendue et la durée de leurs prestations.

Proportionnalité de la collecte des données par les assureurs

Les assureurs ne peuvent recueillir que les données des assurés qui leur sont indispensables à remplir leurs tâches légales (traitement limité au but indiqué ou principe de finalité).

Proportionnalité de la communication des lettres de sortie et des rapports opératoires

Les lettres de sortie comme les rapports opératoires contiennent beaucoup d'informations sensibles. Les informations relatives aux assurés sont soit directement reconnaissables (p. ex. les diagnostics), soit exploitables de manière indirecte (p. ex. il est possible de déduire de la durée de l'anesthésie qu'une personne fume). Il est par conséquent possible de faire ressortir de ces documents d'autres informations qui concernent les maladies ou l'état psychique du patient, lesquelles informations ne sont pourtant pas liées à son hospitalisation ou à son séjour dans un home.

Les assureurs peuvent traiter ces données parce qu'elles leur sont indispensables à déterminer s'ils sont obligés de fournir une prestation. Les hôpitaux et les homes sont par conséquent autorisés à communiquer ces données aux assureurs.

Toutefois, une facture détaillée est en général suffisante pour déterminer l'obligation de l'assureur. Dans des cas particuliers, d'autres indications peuvent par contre se révéler nécessaires.

Manière de procéder recommandée aux hôpitaux et aux homes

Ces considérations conduisent à procéder par étapes, de la manière suivante:

1er degré : Les hôpitaux et les homes établissent une facture détaillée et compréhensible.

2ème degré : Si dans un cas d'espèce, l'assureur a besoin d'indications supplémentaires, il a la possibilité de poser par écrit à l'exécutant de la prestation des questions spécifiques et limitées au cas concret. Il lui incombe de motiver la nécessité de ces questions supplémentaires. Une copie de cette demande est envoyée à la personne assurée à titre d'information.

3ème degré : Si ces informations supplémentaires ne suffisent exceptionnellement pas, l'assureur peut demander une lettre de sortie ou un rapport opératoire à l'intention de son médecin-conseil. Il doit motiver par écrit la nécessité de cette requête. Une copie en est envoyée à la personne assurée à titre d'information.

DSB+CPD.CH / décembre 2001

13.3. Clause de protection des données dans les traités internationaux dans le domaine de la sécurité sociale

Article X

Dans la mesure où des données à caractère personnel sont transmises sur la base de la présente convention, le traitement et la sécurité de ces données sont soumis aux dispositions ci-dessous, conformément à la législation sur la protection des données des parties contractantes applicable au niveau national et international :

a. Les données ne doivent être transmises vers les organes compétents de l'Etat destinataire qu'en vue de l'exécution de la présente convention et des prescriptions légales s'y rapportant. Le destinataire ne les traitera et ne les utilisera que dans le but indiqué. Le traitement à d'autres fins est autorisé dans les limites du droit interne de l'Etat destinataire si ce traitement sert des buts de sécurité sociale, y compris les procédures judiciaires connexes. Par ailleurs, les données ne peuvent être transmises à d'autres organes qu'avec l'autorisation préalable de l'organe transmetteur.

b. Le destinataire informe la partie contractante transmetteuse, à sa demande, de l'utilisation des données transmises et des résultats ainsi obtenus.

c. La partie contractante transmetteuse est tenue de s'assurer de l'exactitude des données à transmettre ainsi que de la nécessité et de l'adéquation au but poursuivi par la communication. Ce faisant, il y a lieu de tenir compte des interdictions de transmission en vigueur d'après le droit national en cause. S'il s'avère que des données inexactes ont été transmises ou que la transmission était indue, le destinataire doit en être avisé immédiatement. Il est tenu de procéder à la rectification ou à la destruction nécessaire.

d. L'organe transmetteur est tenu d'informer de manière appropriée les personnes concernées de la transmission de leurs données personnelles.

e. Les données personnelles transmises ne doivent être conservées qu'aussi longtemps que le requiert le but pour lequel elles ont été transmises et lorsqu'il n'y a aucune raison de supposer que le fait de les effacer porterait atteinte à des intérêts dignes de protection des personnes concernées en matière de sécurité sociale.

f. L'organe transmetteur et le destinataire sont tenus d'inscrire dans leurs dossiers la transmission, la réception et le traitement ultérieur des données personnelles.

g. L'organe transmetteur et le destinataire sont tenus de protéger efficacement les données personnelles transmises contre l'accès non autorisé, les modifications abusives et la communication non autorisée.

13.4. La Poste et la loi sur le blanchiment d'argent

La Poste a le droit de photocopier les documents d'identité

Depuis quelques temps, nous recevons des demandes de la part de titulaires de Comptes Jaunes (anciennement comptes de chèques postaux) qui ont dû – pour certains après plusieurs années – prouver pour la première fois leur identité auprès de la Poste. En qualité d'intermédiaire financier, la Poste est tenue selon la loi sur le blanchiment d'argent (LBA; RS 955.0) de constater l'identité des détenteurs de comptes et de consigner et conserver le contenu des documents d'identité. La pratique de la Poste qui consiste à photocopier les documents est en accord avec les dispositions de la loi sur la protection des données (LPD; RS 235.1).

A l'ouverture d'un nouveau Compte Jaune, la Poste demande au client un passeport ou une carte d'identité qu'elle photocopie. Elle invite également par circulaire tous les titulaires de comptes existants à présenter leurs papiers d'identité au guichet. Ces documents sont également photocopiés par la Poste. Un grand nombre de personnes nous ont contactés pour savoir si cette pratique était conforme à la LPD.

Selon la LPD, un traitement de données personnelles est, entre autres, licite s'il est justifié par la loi (cf. art. 13, al. 1 LPD). Si la Poste demande une copie de la pièce d'identité, elle le fait en tant que mesure préventive contre le blanchiment d'argent en application de la LBA. La Poste étant considérée comme intermédiaire financier au sens de la LBA, elle doit respecter les dispositions de cette dernière. Conformément à l'art. 3 al. 1 LBA, un intermédiaire financier est tenu, au moment où il engage des relations commerciales, d'identifier la partie contractante sur la base d'un document probant. Il doit non seulement examiner la pièce d'identité officielle (telle que carte d'identité ou passeport pour les personnes physiques ou extrait du registre du commerce ou document équivalent pour les personnes morales), il doit également enregistrer le contenu essentiel et le conserver. Il s'agit là d'une obligation de diligence qui concerne toutes les parties contractantes, donc aussi les titulaires de comptes, et qui sert l'intérêt public. La solution choisie par la Poste de photocopier la pièce d'identité correspond en outre à la pratique utilisée dans le domaine bancaire. La procédure consistant à photocopier la pièce d'identité est en outre appropriée et proportionnelle. Au vu de la législation sur la protection des données, le comportement de la Poste ne peut pas être contesté.

Il y a lieu de rendre attentif au fait que la Poste n'est autorisée à utiliser les copies des pièces d'identité que pour le but prévu par la LBA, à savoir la lutte contre le blanchiment d'argent. Cela signifie en d'autres termes que la Poste n'est pas autorisée – par exemple – à vendre ces copies de pièces d'identité à d'autres personnes à des fins de marketing.

13.5. Procédure d'accréditation des autorités de protection des données

PROCEDURE D'ACCREDITATION DES AUTORITES DE PROTECTION DES DONNEESPERSONNELLES ADOPTEE LE 25 SEPTEMBRE 2001 LORS DE LA 23EME CONFERENCE DES COMMISSAIRES A LA PROTECTION DES DONNEES TENUE A PARIS LES 23-26 SEPTEMBRE 2001

Ce document établit la procédure de reconnaissance et des critères d'accréditation des autorités de protection des données personnelles et de la vie privée habilitées à participer à la conférence internationale.

Il se décompose en trois parties :

(A) une partie relative au statut (critères et règles) du comité chargé de l'accréditation (comité de vérification) ;

(B) une partie relative aux principes d'accréditation ;

(C) une partie relative à un avenant aux lignes directrices et procédures relatives aux résolutions de la conférence adopté à la 22eme Conférence.

A. Statut (critères et règles) du comité de vérification

1. Le comité de vérification

Il sera mis en place un comité de vérification («le comité») pour examiner les candidatures des autorités de protection des données personnelles («les autorités») souhaitant être accréditées pour participer à la Conférence Internationale des commissaires à la protection des données personnelles et de la vie privée («la conférence»). Le comité proposera à la conférence les modifications sur son statut (critères et règles) et sur les principes d'accréditation, qu'il estimera nécessaire.

2. Composition du comité

Le comité est composé de trois membres. La composition du premier comité sera déterminée par les participants à session fermée de la 23eme conférence tenue à Paris. Par la suite, les membres du Comité seront choisis uniquement par les autorités accréditées. En procédant ainsi, les participants devront veiller à assurer une diversité dans la composition du comité du point de vue des systèmes juridiques, des zones géographiques et de l'étendu du ressort de compétence. Le comité ne peut pas être composé de plus d'un membre du même pays en même temps.

3. La cooptation

En cas de poste vacant entre les conférences, le comité peut désigner un membre ou des membres parmi les autorités accréditées.

4. Les candidatures à l'accréditation

Les autorités souhaitant être accréditées doivent écrire au comité. Cette demande devra préciser l'ensemble des éléments requis au titre des principes d'accréditation définis au point B.

Les candidatures doivent être présentées dans les trois mois précédant la conférence annuelle. Le comité présentera lors de la conférence une recommandation pour chacune des candidatures reçues et proposera une résolution attestant des éléments d'accréditation pour chaque autorité nationale ou régionale.

Commentaire : les autorités doivent remplir l'une des conditions suivantes, à savoir :

- *Etre une autorité nationale ;*
- *Etre une autorité ayant une compétence régionale (province, canton ou Etat d'un Etat fédéral);*
- *Etre une autorité d'un organisme international ou supranational.*

Le comité peut aussi prendre en compte des demandes émanant d' autorités ayant une compétence moins étendue que celles définies dans les principes d'accréditation. Il peut s'agir d'autorités compétentes dans un secteur d'activité déterminé (le secteur médical par exemple) ou encore d'autorités investi d' une seule mission (exemple : un organisme chargé exclusivement de l'instruction de plaintes ou limité à un rôle de conseil). Ces autorités pourront, à la discrétion de l'hôte de la conférence, être autorisées à participer en tant qu' observateurs mais elles ne disposeront d' aucun droit de vote.

5 La procédure du comité

Le Comité peut adopter toute procédure qui lui semble nécessaire dans l'exercice de ses fonctions.

6. La durée du mandat

Les membres du comité sont nommés pour une durée de deux ans renouvelable une fois. Les membres cooptés sont nommés pour la période restant à courir jusqu'à la prochaine conférence.

7. Les frais

Les membres devront supporter leurs propres frais.

8. Les mises à jour des accréditations

A la demande de chacune des autorités accréditées, le comité peut réexaminer la candidature d'une autorité précédemment accréditée. Il proposera une recommandation précisant que l'accréditation doit être ou non maintenue.

B. Principes d'accréditation

Les autorités accréditées sont celles qui en vertu de l'étendu de leur mission et de leur grande expérience, sont les premiers experts en matière de principes et de pratiques relatives à la protection des données personnelles et de la vie privée dans leur ressort. Elles ont le mandat précis de promouvoir et d'assurer la protection des données personnelles et de la vie privée dans une large sphère d'activité et doivent disposer de l'ensemble des pouvoirs nécessaires pour assurer leurs missions.

1. Les fondements juridiques

L'autorité de protection des données doit être une autorité publique instituée par un dispositif juridique.

Commentaire : Le fondement juridique qui institue cette autorité doit prévoir son indépendance, et permettre d'assurer ses fonctions ainsi que démontrer son engagement à assurer une protection effective. L'encadrement juridique doit être celui du type qui régit habituellement les organismes publics significatifs chargés des droits des citoyens dans son ressort. Ce sera normalement une législation, cependant selon les traditions locales, une mesure réglementaire adaptée peut être appropriée. Le cadre légal doit être transparent et avoir une permanence suffisante afin qu'il ne puisse pas être révoqué ou changé sans en référé au pouvoir législatif.

2. Autonomie et indépendance

L'autorité de protection des données doit, pour le bon exercice de ses missions, bénéficier de garanties lui permettant d'agir en pleine autonomie et indépendance.

Commentaire : L'autonomie exige que l'autorité soit en mesure sur le plan juridique et pratique d'initier et de mener les actions nécessaires sans avoir à en obtenir l'autorisation. L'indépendance est essentielle afin que les autorités puissent agir librement des interférences politiques ou gouvernementales et pour qu'elles puissent résister aux pressions des groupes d'intérêts. Les principales garanties sont *:*

- *nomination pour une durée déterminée ;*
- *révocation du mandat aux seuls motifs suivants, à savoir incapacité à exercer ses fonctions, négligence le travail ou mauvaise conduite caractérisée ;*

- *pouvoir rendre-compte directement auprès du chef du gouvernement ou du parlement et disposer d'une liberté de parole dans son domaine de compétence ;*
- *immunité contre les poursuites personnelles relatives aux actes effectués dans le cadre de leur fonctions ;*
- *disposer d'un pouvoir d'investigation.*

3. Conformité avec les textes internationaux

La législation dont relève l'autorité doit être compatible avec les principaux textes internationaux existants en matière de protection des données personnelles et de la vie privée.

Commentaire : Les principaux textes internationaux sont : les lignes directrices de l'OCDE (1980), la Convention n°108 du Conseil de l'Europe (1981), les lignes directrices de l' ONU (1990), la directive européenne 95/46 (1995), et, dans la mesure où ils sont pertinents, les principes de l'ONU relatif au statut et au fonctionnement des institutions nationales chargées de la protection et de la promotion des droits de l'homme (1995).

4. Les compétences appropriées

L'autorité doit être investie d'une série de missions et disposer des pouvoirs nécessaires pour les assurer.

Commentaire : Une autorité de protection des données personnelles doit avoir une série de missions dans les domaines tels que la mise en conformité, la surveillance, l'investigation, la réparation, le conseil et l'information auprès du public. Cette autorité ne doit pas uniquement avoir un rôle consultatif mais disposer d'un pouvoir de surveillance ayant des conséquences légales ou administratives.

C. Avenant aux lignes directrices et procédures relatives aux résolutions de la conférence

Lors de la 22eme conférence de Venise en septembre 2000, les commissaires ont adopté des lignes directrices et procédures relatives aux résolutions de la conférence. L'avenant suivant est adopté pour les prochaines résolutions : 1. Lors de la 24eme Conférence Internationale, la réunion des autorités examinera tout d'abord les recommandations faites par le comité de vérification et elle décidera de les approuver ou de les rejeter. Par la suite, les résolutions pourront uniquement être proposées et approuvées par les autorités accréditées (que celles-ci aient une compétence nationale ou régionale).

2. A partir de la 24eme Conférence Internationale, seules les autorités accréditées auront compétence pour adopter des résolutions. Une résolution ne peut être adoptée que si la majorité des autorités accréditées disposant d'un droit de vote sont présentes. Dans la mesure du possible les résolutions sont adoptées par consensus plutôt que selon une procédure de vote formel. Lorsqu'un vote est nécessaire, chaque pays dispose d'une voix et la résolution est adoptée à la majorité simple des pays présents. Dans le cas où il y aurait plus d'un représentant d'un même pays, le vote est effectué par l'autorité nationale qui doit recueillir préalablement l'avis des autorités régionales de ce pays, lesquelles ont en tout état de cause la possibilité de faire connaître leur point de vue. Si cette autorité nationale n'est pas représentée, les autorités régionales de ce pays présentes à la conférence peuvent décider de la procédure de vote. A défaut d'accord, le vote sera annulé. Les autorités d'un organisme international ou supranational qui ont été dûment accréditées peuvent participer aux réunions et contribuer aux travaux mais elles n'ont pas le droit de vote sauf si la Conférence leur a conféré des droits de vote lors de leur accréditation.

3. Les propositions de résolutions présentées par le comité de vérification relatives aux accréditations des autorités de protection des données personnelles sont communiquées avant la conférence dans les délais prévus par les Lignes directrices et Procédures relatives aux résolutions de la Conférence adoptées le 29 septembre 2000, lors de la 22ème conférence tenue à Venise. Cependant, en cas d'urgence, la conférence peut renoncer à cette exigence.

13.6. Recommandations du PFPD

13.6.1. Recommandation concernant la communication de données personnelles extraites de demandes d'ouverture de comptes

Voir page 124 de la partie en langue allemande.

13.6.2. Recommandation concernant les formulaires d'inscription pour les appartements à louer

Voir page 128 de la partie en langue allemande.

13.6.3. Transmission à la Commission fédérale de la protection des données de la recommandation concernant le dépistage de la consommation de drogues chez les apprentis

Voir page 135 de la partie en langue allemande.

13.6.4. Recommandation concernant le CD-ROM «Black Book»

Voir page 151 de la partie en langue allemande.