

Message concernant la loi fédérale sur la protection des données (LPD)

du 23 mars 1988

Messieurs les Présidents, Mesdames et Messieurs,

Nous vous soumettons un message à l'appui du projet de loi fédérale sur la protection des données, en vous proposant de l'adopter.

Nous vous proposons en outre de classer les interventions parlementaires suivantes:

- | | |
|---------------|--|
| 1971 P 10.898 | Législation sur l'ordinateur (N 11. 12. 72, Bussey) |
| 1977 P 77.381 | Centres d'informations publics et privés (N 17. 1 78, Carobbio) |
| 1982 P 86.336 | Offres d'emploi et protection de la personnalité
(N 8. 10. 82, Crevoisier) |
| 1984 P 84.598 | Protection de la personnalité du salarié (N 22. 3. 85, Reimann) |
| 1984 P 84.909 | Protection des données. Régime transitoire
(N, non encore traitée, Leuenberger) |

Nous vous proposons également de ne pas donner suite aux initiatives parlementaires suivantes:

- | | |
|-------------|---|
| 1977 77.223 | Fichiers personnels et protection de la personnalité. Constitution (non encore traitée, Gerwig) |
| 1977 77.224 | Fichiers personnels et protection de la personnalité. Loi (non encore traitée, Gerwig). |

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames et Messieurs, l'assurance de notre haute considération.

23 mars 1988

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Stich

Le chancelier de la Confédération, Buser

Condensé

Suite à l'avènement de l'informatique et des technologies des télécommunications, suite à la multiplication des traitements de données, suite à la diffusion d'informations personnelles toujours plus nombreuses au sein de la société, de l'économie et de l'Etat, les risques d'atteinte à la personnalité ont considérablement augmenté. Dans leur état actuel, le droit privé et le droit administratif communs ne sont plus en mesure d'offrir la protection adéquate. La législation qui fait l'objet du présent message, entend remédier à cette déficience, autrement dit, offrir une protection efficace aux personnes concernées par les traitements de données.

Notre projet de loi renferme dans sa partie générale les principes fondamentaux applicables au traitement de données, qu'il soit le fait d'organes de la Confédération ou de personnes privées. Il accorde en outre à tout-un-chacun le droit d'exiger du maître d'un fichier des renseignements sur les données recueillies sur son compte; à cette fin, la plupart des fichiers devront être enregistrés. Cette obligation est plus étendue pour les organes fédéraux que pour les personnes privées, lesquelles ne devront déclarer que les seuls fichiers présentant, du point de vue de la protection de la personnalité, des risques particuliers. Enfin, certaines catégories de communications de données à l'étranger seront soumises à déclaration préalable, et ce, en fonction de la quantité et de la nature des informations transmises.

La partie du projet qui est consacrée aux traitements de données effectués par des personnes privées complète et concrétise la protection de la personnalité instituée par le code civil. D'une part, elle exemplifie certains traitements de données susceptibles de porter atteinte à la personnalité. D'autre part, elle fournit au juge certains éléments qui lui permettront d'apprécier dans quels cas les intérêts de celui qui traite des données doivent être considérés comme prépondérants et, partant, l'atteinte à la personnalité comme justifiée. A cet égard, le présent projet tient amplement compte des besoins d'informations de l'économie. Relevons enfin qu'il appartiendra au juge civil de se prononcer sur les litiges portant sur les traitements de données effectués par des personnes privées.

La loi réglemente ensuite, dans le détail, les traitements de données effectués par l'administration fédérale et les autres organes fédéraux. Elle établit les responsabilités en matière de protection des données et détermine à quelles exigences légales doivent répondre les différents traitements envisageables. Elle précise en outre à quelles conditions les organes fédéraux sont en droit de collecter des données, de les communiquer ou de procéder à d'autres formes de traitements. A ce propos, on relèvera que les intérêts spécifiques des organes chargés de la sûreté de l'Etat et de la sûreté militaire n'ont pas été oubliés.

Un préposé fédéral à la protection des données sera appelé à surveiller l'application de la loi. Il pourra conduire des enquêtes; reste que, s'agissant de personnes privées, il ne pourra intervenir que dans des cas particuliers. Quoi qu'il en soit, il ne sera pas en droit de prendre des mesures contraignantes: il ne pourra faire que des recommandations. Cela dit, il lui sera toujours possible de soumettre une affaire pour décision à la

Commission fédérale de la protection des données. Cette institution connaîtra en outre les litiges en matière de protection des données, qui surviennent entre les administrés et l'administration. Ses décisions pourront être déférées au Tribunal fédéral.

Le projet règle aussi la communication de données à des fins de recherche médicale. Des données soumises au secret professionnel, tel le secret médical, ne pourront être communiquées qu'avec le consentement des personnes concernées ou moyennant l'autorisation d'une Commission d'experts nommée par le Conseil fédéral. Celle-ci n'est cependant en droit d'octroyer une telle autorisation qu'à certaines conditions: la recherche ne peut être effectuée avec des données rendues anonymes et il est impossible ou particulièrement difficile pour le chercheur d'obtenir le consentement des intéressés; au demeurant, les intérêts de la recherche doivent primer les intérêts au maintien du secret. Cette réglementation, conçue pour l'essentiel comme un complément au code pénal, doit concilier deux intérêts divergents: la protection de la personnalité du patient d'une part et l'intérêt public à une recherche médicale efficiente de l'autre.

Notre projet prévoit également de réviser la procédure pénale fédérale et la loi sur l'entraide pénale internationale, en vue d'y consacrer certains principes du droit de la protection des données; ces principes régiront notamment l'enquête préliminaire et l'échange d'informations avec INTERPOL.

En se dotant d'une législation sur la protection des données, la Suisse suit l'exemple de presque tous les Etats industrialisés. Signalons enfin que notre projet concrétise nombre de principes de protection des données consacrés par le droit international public. Partant, il contribue à favoriser les échanges internationaux d'informations.

Message

1 Partie générale

11 Nécessité d'une législation sur la protection des données

111 Remarques liminaires

La collecte et le traitement des données mettent en jeu la personnalité des individus, suscitant des réactions plus ou moins variables en fonction de leur propre sensibilité: certains considèrent que les activités d'information favorisent la communication entre individus, d'autres par contre s'estiment lésés, voire entravés dans leurs facultés d'épanouissement.

Le traitement de données personnelles peut porter préjudice aux personnes concernées de différentes manières. L'ignorance désécurise: s'il est inquiétant de ne pas savoir quelles données vous concernant sont traitées, il l'est encore plus de ne pas connaître quelle image votre entourage se fait de vous¹⁾). En outre, nombre de personnes s'offusquent de ce que l'on ose recueillir secrètement des informations sur leur compte²⁾. Enfin, il est incontestable que les décisions prises sur la base d'informations inexactes, incomplètes ou périmées sont susceptibles de léser les personnes concernées ou, à tout le moins, de leur causer du tort³⁾. Un individu peut pâtir sa vie durant de la réutilisation d'une information péjorative conservée indéfiniment. Mais ce ne sont pas là les seuls cas d'atteintes. Il y en a encore bien d'autres, à commencer par les traitements excessifs de données, l'étalage injustifié d'un passé compromettant⁴⁾, ou encore, dans le cadre d'une relation contractuelle, la collecte de données relatives à son partenaire, mais absolument inutiles à la réalisation de l'affaire. Enfin, on ne saurait nier que les services administratifs, en accumulant et en échangeant sans limites des données personnelles, risquent de porter préjudice à la personnalité des administrés⁵⁾. Finalement, personne n'apprécie l'usage de données dans un but autre que celui pour lequel elles ont été recueillies. Ainsi, par exemple, des informations sur les relations de travail ou sur des mesures sociales ne devraient pas être réutilisées hors de leur contexte.

112 Croissance des flux d'informations et développement des nouvelles technologies

Depuis la deuxième guerre mondiale, non seulement on utilise toujours plus d'informations personnelles, mais encore leur traitement a revêtu de nouvelles formes. L'accroissement du nombre des transactions commerciales, l'apparition de nouvelles stratégies de vente et de nouvelle méthodes de gestion d'entreprise, l'extension et la diversification du crédit bancaire exige des quantités toujours plus importantes d'informations personnelles, lesquelles sont exploitées suivant des techniques toujours plus complexes. Le secteur public n'est pas demeuré en reste: la multiplication des tâches étatiques et les exigences plus grandes quant à la

^{*)} La note ¹⁾ comme les autres notes figurent à la fin du message.

qualité des prestations ont conduit à une importante augmentation des traitements d'informations.

L'avènement de la société d'information que nous connaissons aujourd'hui n'aurait pas été possible sans l'apparition de l'informatique et des nouvelles techniques de télécommunication. Les installations de traitements automatisés de données permettent en effet d'exploiter les informations avec une systématique et une efficacité inconnues jusqu'alors. A l'heure qu'il est, on est en mesure de collecter, de réunir, de traiter et de diffuser des informations presque sans aucune limite. La technologie moderne permet de connecter des fichiers entre eux, de les fractionner, de les exploiter et d'en transmettre le contenu à volonté. Ces possibilités de traitement devraient encore augmenter avec l'essor de la télématique, c'est-à-dire l'union du traitement automatisé des données et des techniques de télécommunication. Plus rien ne s'oppose à la création de réseaux locaux, régionaux et internationaux connectant des centres de calcul et des ensembles de données géographiquement éloignés.

Les nouvelles technologies permettent d'exercer une surveillance plus étroite des personnes, notamment de leur comportement. Cette surveillance n'est pas seulement le fait d'enregistrements vidéo, mais aussi de moyens toujours plus sophistiqués de contrôle automatisé de l'accès, du temps de présence, des performances et des communications. L'utilisation d'appareils électroniques, le franchissement d'enceintes de sécurité ou la lecture automatisée de cartes d'identité ou de crédit permettent de récolter toute une série d'informations. Il en va de même des systèmes de communication bidirectionnels et automatisés tel le Vidéotex. A la saisie traditionnelle au clavier se substitue de plus en plus la lecture optique d'images, de textes, voire d'autres signes, ou l'enregistrement de sons.

Conséquences de cette évolution: les risques de porter atteinte à la personnalité se sont accrus. En particulier l'individu n'est souvent plus en mesure de déterminer, même de manière approximative, quelles données le concernant sont traitées, par qui, où et quand. La maîtrise de ses propres données, il l'a perdue, et, avec elle, la faculté de choisir les personnes avec lesquelles il souhaite entrer en communication et ce qu'il entend leur faire savoir à son sujet. Plus grave, souvent il n'est plus à même de reconnaître les erreurs et les abus engendrés par les traitements d'informations, et d'en découvrir les responsables.

Mais, le traitement automatisé des données revêt aussi du point de vue de la protection des données des aspects positifs. Il permet notamment de rendre anonymes les données personnelles à peu de frais.

113 Objectifs principaux de la loi sur la protection des données

Le but d'une loi sur la protection des données n'est pas de stopper le développement des technologies de l'information; ni même de limiter les possibilités qu'elles offrent. Ces technologies ont incontestablement fait leurs preuves; et ce, dans des domaines aussi divers que les sciences, l'économie ou l'administration. Les progrès dont on leur est redevable ne sauraient être remis en cause; bien au contraire, il faut qu'ils se poursuivent. Néanmoins, il est impératif de consacrer certains principes directeurs garantissant qu'aucun traitement de données inutile

ou indésirable ne vienne menacer l'épanouissement de la personnalité des individus. A moins que l'ordre juridique n'en dispose autrement, chacun doit pouvoir déterminer la valeur qu'il attache à ses propres données et l'utilisation qu'il souhaite qu'on en fasse. Chaque individu doit pouvoir déterminer librement le cercle des personnes avec qui il souhaite entrer en communication et sous quelle forme⁶⁾.

Cela signifie, en premier lieu, que la vie privée et familiale doit être à l'abri des atteintes. Ainsi, seuls les particuliers ou les services publics qui font valoir un intérêt prépondérant devront être en droit de collecter des informations concernant la sphère privée d'une personne⁷⁾. En outre, les opinions religieuses, philosophiques et politiques, requièrent une protection spécifique, car elles relèvent des droits fondamentaux que sont la liberté de croyance et de conscience, la liberté d'opinion, le droit de vote et de pétition. Une loi sur la protection des données a aussi pour but d'empêcher que l'individu ne soit réduit à l'état de simple objet d'information: l'individu doit pouvoir déterminer l'image et les informations que son environnement aura de lui. Aussi peut-il revendiquer le droit de savoir qui détient des données à son sujet et dans quel but elles sont traitées. A défaut, il ne sera pas en mesure de se déterminer de manière adéquate au cours de ses activités privées ou professionnelles ou tout simplement en société. On lui accordera également le droit de faire corriger ou détruire des informations le concernant, ou d'exiger que celui qui traite ces informations les garde secrètes.

114 L'état du droit suisse

114.1 Le secteur privé

A l'heure actuelle, la protection des données en droit privé se fonde sur les seuls principes de la protection générale de la personnalité, telle qu'elle est instituée par les articles 28 et suivants du code civil (CC). Aux termes de l'article 28, 1^{er} alinéa, du code civil, entré en vigueur le 1^{er} juillet 1985, «Celui qui subit une atteinte illicite dans sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe». La notion de personnalité doit être entendue dans un sens large, couvrant l'ensemble des valeurs physiques, psychiques, morales et sociales liées à l'existence de l'individu⁸⁾. Cette définition extensive laisse cependant une question fondamentale en suspens: dans quels cas y a-t-il effectivement une atteinte illicite à la personnalité? De surcroît, la loi ne donne aucune indication permettant de déterminer quels traitements de données sont licites.

La jurisprudence, il est vrai, a posé quelques jalons et défini quelques critères. Ainsi, il y aura atteinte à la personnalité si le traitement d'informations vient à menacer la sphère privée ou intime⁹⁾. La *sphère intime* comprend tous les faits et les événements de la vie dont seule a connaissance la personne concernée ou des personnes jouissant de sa confiance. A la *sphère privée* appartiennent les autres faits de la vie privée qui ne doivent pas être portés à la connaissance d'un large public. Constituent également des violations de la personnalité les atteintes à l'honneur et à l'image sociale, ainsi que les traitements de données personnelles

inexactes, s'ils donnent une image fausse de la personne concernée¹⁰⁾. En résumé, la jurisprudence est d'avis qu'un traitement de données est illicite s'il porte atteinte à un aspect de la vie de l'individu, à son indépendance morale ou à son crédit social.

Autant dire qu'actuellement les traitements de données sont réglementés de manière très sommaire; désireuses de pourvoir à la protection des données par des normes plus précises, quelques *organisations privées* ont, de manière isolée, pris l'initiative d'édicter des règles dans ce domaine. Tour à tour, la Conférence des instituts suisses d'études de marché et d'opinion, en collaboration avec l'Association suisse des spécialistes en études de marché, l'Association d'agences de renseignements commerciaux en Suisse et l'Association suisse de vente par correspondance ont élaboré des règles déontologiques applicables aux traitements de données personnelles qu'ils effectuent. On ne manquera pas non plus de signaler les «Nouveaux principes à l'usage des médecins-conseil» et les «Règles fondamentales pour les médecins d'entreprise» adoptés par la Chambre médicale suisse en 1981. Mentionnons enfin deux textes importants définissant des principes destinés à assurer la protection des données: premièrement l'accord passé en 1983 entre l'Association patronale suisse des constructeurs de machines et industriels en métallurgie (AFM) et la Fédération des travailleurs de la métallurgie et de l'horlogerie (FTMH), secondement la Convention modèle de 1984 de la Commission des employés de l'Union syndicale suisse intitulée «Nouvelles techniques et protection des données dans l'entreprise».

114.2 Le secteur public

A l'instar des règles sur la protection de la personnalité consacrées par le droit civil, le droit constitutionnel offre également une certaine protection contre les traitements de données, illicites ou excessifs. Cette protection ne découle pas d'une disposition constitutionnelle topique, mais, d'une part, d'un droit constitutionnel non-écrit: la liberté personnelle, et, d'autre part, de l'article 8 de la Convention européenne des droits de l'homme (CEDH). Liberté cardinale, la liberté personnelle garantit non seulement «le droit d'aller et venir et le droit au respect de l'intégrité corporelle», mais aussi «toutes les libertés élémentaires... dont l'exercice est indispensable à l'épanouissement de la personne humaine, notamment... le droit d'apprécier une situation et de se déterminer en conséquence»¹¹⁾. Aux termes de l'article 8 de la CEDH, «Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance». De surcroît, le secret du vote et le droit de pétition imposent certaines limites au traitement des informations; il s'agit d'éviter que le nom des signataires d'initiatives, de référendums ou de pétitions soit utilisé à des fins politiques ou policières¹²⁾. Relevons enfin que l'article 4 de la constitution (cst.), revêt ici une signification nouvelle: il permet à la personne concernée d'être partie prenante au traitement de données¹³⁾.

Afin de concrétiser ces principes, le Conseil fédéral a édicté le 16 mars 1981 des «Directives applicables au traitement de données personnelles dans l'administration fédérale»¹⁴⁾ et, ce, à titre provisoire, car les travaux préparatoires à la loi sur

la protection des données avaient déjà débuté. Ces directives posent les principes juridiques appelés à régir les traitements de données et font à l'administration fédérale obligation de renseigner les personnes concernées. Elles sont destinées à familiariser l'administration avec les impératifs de la protection des données et, par la même, à préparer le terrain à l'entrée en vigueur de la future loi. Parant au plus pressé, le Conseil fédéral a en outre soumis certains grands systèmes d'information de la Confédération à des règles de protection des données. Mentionnons, à titre d'exemple, l'ordonnance du 20 octobre 1982 sur le Registre central des étrangers (RS 142.215), l'ordonnance du 16 décembre 1985 sur le système de recherches informatisées de police (RIPOL; RS 172.213.61), l'ordonnance du 29 octobre 1986 sur les contrôles militaires (PISA; RS 511.22), l'ordonnance du 27 septembre 1982 concernant les tests d'application d'un système d'information en matière de placement et de statistiques du marché du travail (RS 823.114), ainsi que plusieurs ordonnances régissant la statistique fédérale¹⁵.

Quelques cantons disposent déjà d'une législation sur la protection des données applicable au secteur public. Le pionnier fut assurément le canton de Genève qui s'est doté dès 1976 d'une «loi sur la protection des informations traitées automatiquement par ordinateur»; ce texte a fait l'objet d'une révision totale en 1981. D'autres cantons – Vaud, Neuchâtel, Valais, Berne, Jura, Tessin et Thurgovie – ont suivi l'exemple genevois. Les cantons de Bâle-Ville, Bâle-Campagne, Glaris, Lucerne, Saint-Gall, Soleure et Zurich, quant à eux, sont actuellement en train de préparer leur loi sur la protection des données. Ailleurs, on se contente provisoirement d'ordonnances ou de simples directives.

114.3 Insuffisance du droit en vigueur

Nous venons de le voir, notre ordre juridique renferme déjà certaines dispositions régissant le traitement d'informations. Toutefois, en dépit de quelques décisions judiciaires significatives, nous sommes dépourvus d'une protection efficace contre les atteintes causées par les traitements d'informations. Ni le droit privé, ni le droit public ne sont en mesure de prendre suffisamment en compte ce besoin de protection, besoin particulièrement aigu à l'heure de l'informatique.

S'agissant de traitements relevant du droit privé, le caractère insuffisant du droit en vigueur tient avant tout au fait que les personnes concernées ne peuvent, la plupart du temps, déterminer quelles personnes traitent des données à leur sujet. Si elles y parviennent, il est loin d'être certain qu'elles puissent obtenir des renseignements sur les fichiers qui les concernent et les données qu'ils renferment. De plus, elles sont difficilement en mesure d'identifier les risques qu'elles courent ou les atteintes qu'elles subissent. L'article 28 du code civil, de par sa formulation très générale, ne leur fournit en effet aucun critère permettant de déterminer si un traitement est licite ou illicite. En outre, la personne concernée éprouve souvent les pires difficultés à établir le lien de causalité adéquate entre un traitement d'informations et l'atteinte portée au droit de la personnalité. Dans ces conditions, on comprend que la personne concernée hésite le plus souvent à saisir la justice, car l'issue du procès est des plus aléatoires.

La jurisprudence relative aux droits fondamentaux n'affecte les traitements de données effectués par les organes étatiques que d'une façon limitée et ponctuelle¹⁶). De surcroît, les tâches de l'administration impliquant le traitement d'informations ne sont en général définies que de manière très fragmentaire. Certes, il ne manque pas de dispositions contraignant les administrés à fournir les informations aux autorités, réglant l'utilisation de données qu'elles détiennent ou encore leur imposant des obligations d'entraide. Cependant, ces dispositions répondent en général uniquement aux finalités propres de la loi qui les renferment. Leur but premier n'est donc pas la protection des personnes concernées. Le devoir de discrétion imposé aux agents de la fonction publique fait certes obstacle, dans une certaine mesure, à la communication d'informations à des particuliers. Il ne réglemente néanmoins pas de façon adéquate l'entraide administrative ou judiciaire. En outre, aucune règle n'interdit à ce jour à l'administration publique d'utiliser des données à des fins autres que celles initialement prévues. Aucune règle non plus ne vient préciser dans quelle mesure une collecte de données est conforme aux impératifs de la protection des données. Font également défaut, mais en droit public cette fois, des procédures administratives ou judiciaires permettant aux administrés de s'informer sur les données les concernant, d'en contrôler leur utilisation ou leur communication et de se défendre contre les erreurs de traitement¹⁷).

115 Différences dans la recherche médicale entre le droit en vigueur et la pratique

115.1 Protection des données et recherche médicale: des intérêts divergents

Les informations sur l'état de santé, telles les données afférentes aux maladies ou aux infirmités graves, font partie de ces données très sensibles qui appartiennent par excellence à la sphère intime. On comprend dès lors que bien des personnes hésitent à donner à des tiers des informations sur leur santé. Elles craignent que leur situation sociale ou leur avenir professionnel n'en pâtisse. Il en va tout autrement dans une relation d'ordre médical. Convaincu que le rétablissement est à ce prix, le patient donne au personnel soignant foule d'informations intimes sur son état physique et psychique. Ces informations, il les communique sans hésitation aucune, pour autant qu'il ait confiance dans le personnel soignant, à commencer par son médecin. La pierre angulaire de cette relation de confiance est la conviction que la plus grande discrétion entourera les constatations faites en cours de traitement.

Il n'y a là rien de nouveau. L'une des plus anciennes règles de protection des données vise justement le domaine de la santé; cette règle n'est autre que le secret professionnel du médecin consacré par le serment d'Hippocrate. Aujourd'hui, la plupart des pays sanctionnent pénalement la violation du secret médical. Il en est de même en Suisse: l'article 321 du code pénal (CP) punit, sur plainte, de la prison ou de l'amende le médecin, le dentiste, le pharmacien ou la sage-femme qui révèle un secret professionnel; quant à leurs auxiliaires, ils sont passibles de la même peine. Ces personnes ne peuvent être déliées du secret professionnel qu'avec le

consentement du patient ou l'autorisation de l'autorité supérieure ou de l'autorité de surveillance. La recherche médicale requiert par ailleurs quantité de données personnelles. Plus que tout autre secteur de la recherche scientifique, elle ne peut se passer d'informations permettant d'identifier les personnes concernées. Seules des données personnelles permettent, par exemple, de faire bénéficier immédiatement une personne en traitement des fruits d'une recherche, de reconnaître des enregistrements répétés de personnes, d'organiser des groupes de comparaison, d'entreprendre des examens de longue durée ou de poser des questions complémentaires. Cette activité de recherche médicale répond à un intérêt public et/ou privé important. La lutte contre les affections graves ou très répandues en dépend; en outre dans nombre de cas, la recherche médicale a grandement concouru au succès d'une thérapie ou de mesures prophylactiques. Dès lors, on ne saurait nier qu'elle est au service de la santé publique.

115.2 Réglementation insuffisante dans le code pénal

Les dispositions pénales sur le secret professionnel (art. 321 CP) ne sont pas toujours scrupuleusement respectées dans la pratique. Elles ne tiennent en effet pas compte des récents développements de la recherche médicale.

Selon le droit en vigueur, le chercheur doit obtenir le consentement des patients, directement ou par l'intermédiaire du médecin traitant, avant de consulter leurs dossiers médicaux¹⁸⁾. Reste qu'il n'est pas toujours aisé d'obtenir cet accord: les patients concernés peuvent avoir disparu sans laisser de trace ou être décédés, voire simplement résider à de grandes distances les uns des autres. Que les données protégées par le secret professionnel soient communiquées à une personne elle aussi astreinte au secret professionnel ne change rien: même l'échange d'informations entre médecins constitue une violation du secret professionnel. Il s'ensuit que le secret médical doit également être respecté au sein d'un seul et même hôpital; la communication d'informations sur le compte d'un patient aux différentes personnes participant à son traitement fait bien entendu exception. Dans ce cas particulier, on admet que le patient a tacitement consenti à la levée du secret médical¹⁹⁾. Si le patient doit dès le début de son hospitalisation compter sur le fait que son dossier médical parviendra, tout au long du traitement, à la connaissance de plusieurs personnes, il ne sera, généralement, pas à même de déterminer l'identité de tous ceux qui seront mis au courant. Eu égard à l'organisation et aux structures d'un établissement hospitalier, il se justifie en outre de tenir pour licite toute communication de données, relatives à des patients, au sein du personnel hospitalier relevant de la même direction thérapeutique – soit, le plus souvent, de la même division hospitalière.

116 La protection des données à l'étranger

Dès la fin des années 60, les Etats industriels occidentaux se sont dotés de législations sur le traitement de données personnelles. La première loi sur la protection des données a vu le jour en 1970 dans le Land de Hesse. Caractéristique principale de ce texte: l'institution d'une instance de contrôle entièrement

indépendante de l'administration et responsable devant le seul Parlement. En 1973, c'était au tour de la Suède d'adopter une loi sur la protection des données, laquelle soumet à autorisation de l'«Inspectorat des données» la création et l'exploitation de fichiers électroniques de données personnelles. La République fédérale d'Allemagne devait adopter une loi sur la protection des données en 1977; les Länder lui emboîtèrent le pas et adoptèrent, dans leurs domaines de compétences, leurs propres lois. En 1978, le Parlement français votait la «Loi relative à l'informatique, aux fichiers et aux libertés». La même année, l'Autriche, la Norvège et le Danemark se dotaient également de lois sur la protection des données; ce dernier pays alla même jusqu'à édicter deux textes différents, l'un pour le secteur privé, l'autre pour le secteur public. Ces trois pays ne furent pas les derniers. Le Luxembourg suivait en 1979, l'Islande, Israël et la Hongrie – par voie de décret – en 1981, la Grande-Bretagne en 1984 et tout dernièrement, en 1987, la Finlande et l'Irlande.

L'évolution législative outre-mer n'est pas non plus dénuée d'intérêt. En 1974, les Etats-Unis d'Amérique ont adopté une loi fédérale qui accorde aux personnes concernées un droit d'accès et limite clairement les possibilités de traitement de données effectués par l'administration. Cette loi, qui s'applique uniquement aux autorités fédérales, est complétée par des lois spéciales régissant la protection des données dans certains secteurs, notamment le crédit, l'éducation et la formation, les moyens électroniques de paiement et les systèmes de télécommunications. Les Etats fédérés ne sont pas demeurés en reste: s'inspirant parfois de lois-modèles, ils se sont dotés de leur propre réglementation, valable tant pour le secteur public que pour le secteur privé. Le Canada et l'Australie ont eu une évolution semblable. On relèvera enfin que dans ces deux pays, comme aux USA, l'Etat fédéral ne dispose que de compétences limitées de réglementer le secteur privé.

Les législations américaine, canadienne et australienne ont une caractéristique commune: toutes trois ont cherché à concilier le droit de la personnalité et de la protection des données avec des dispositions sur la publicité de l'administration et sur l'accès aux informations détenues par les autorités. Cela dans le but de pondérer deux intérêts divergents: la nécessité du secret et les besoins de transparence. Au Canada, la loi de 1982 édictant la loi sur l'accès à l'information et la loi sur la protection des renseignements personnels atteignent cet objectif.

117 La protection internationale des données

L'avènement de l'informatique et des réseaux modernes de télécommunications a non seulement permis de développer fortement les relations commerciales, mais encore de favoriser une coopération étroite des Etats et des organisations internationales. Les activités publiques ou privées dans lesquelles le traitement de données s'arrête aux frontières nationales ont tendance à diminuer. Fortes de ce constat, plusieurs organisations internationales se sont soucies de régler les flux transfrontières de données par des normes de droit international public²⁰.

La réglementation la plus étendue en la matière est le fait du *Conseil de l'Europe*. Ouverte à la signature des Etats-membres le 28 janvier 1981, sa «Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des

données à caractère personnel» a déjà été ratifiée par la République fédérale d'Allemagne, l'Autriche, la France, l'Espagne, la Grande-Bretagne, le Luxembourg, la Norvège et la Suède. Elle a en outre été signée par dix Etats.

La Convention entend garantir les libertés fondamentales, notamment la vie privée des personnes physiques lors du traitement automatisé de données personnelles. Les Etats contractants s'obligent à instituer dans leur droit interne les garanties minimales de protection des données énoncées aux articles 4 à 11. Il en résulte une harmonisation des diverses réglementations de protection des données consacrées par les Etats cocontractants, laquelle facilite les flux transfrontières d'informations (art. 12). Enfin, la Convention règle la coopération et l'entraide internationales entre les parties (art. 13 à 17). Relevons en outre que le Conseil de l'Europe a également élaboré plusieurs *Recommandations* appelées à régir la protection des données dans certains domaines particuliers, à savoir les banques de données médicales automatisées, la recherche et la statistique, le marketing direct, la sécurité sociale et la police.

Pour sa part, l'*Organisation de Coopération et de Développement Economique* (OCDE) a édicté des *«Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel»*. Ce texte, accompagné d'une Recommandation, a été transmis le 23 septembre 1980 aux gouvernements des pays membres; tous l'ont accepté. Les lignes directrices posent les principes généraux applicables aux flux internationaux de données et à la protection des données; en particulier, elles recommandent aux Etats-membres de collaborer lors de l'échange international de données. Signalons enfin que ces lignes directrices revêtent une signification particulière: d'une part elles ont été approuvées par les Etats-Unis, le Canada, le Japon et l'Australie, d'autre part, un grand nombre d'entreprises multinationales se sont engagées publiquement à les appliquer.

12 Les impératifs d'ordre constitutionnel

La constitution ne contient aucune disposition expresse qui habilite la Confédération à légiférer en matière de protection des données. Certes, la protection des données vient concrétiser de manière substantielle les droits fondamentaux traditionnels et renforcer leur impact; la doctrine dominante souligne toutefois que ceux-ci ne sont pas à eux seuls attributifs de compétences. Cela dit, la Confédération peut adopter des dispositions de protection des données sur la base de certaines compétences législatives dont elle dispose déjà.

121 Le droit privé

L'article 64 cst. autorise la Confédération à légiférer en matière de droit privé. Se fondant sur cette disposition, le législateur fédéral peut étendre et renforcer la protection de la personnalité qui n'est actuellement consacrée que de manière générale *par des dispositions de droit privé régissant spécifiquement la protection des données*. De surcroît, il peut également prévoir des dispositions qui, bien qu'elles revêtent un caractère de droit public, – par exemple l'obligation de déclarer

certaines fichiers – sont nécessaires à l'exécution et à l'application uniforme du droit civil fédéral, ou encore permettent d'éviter des conflits de lois²¹⁾.

En outre, sur la base de l'article 31^{bis}, 2^e alinéa, cst., la Confédération peut édicter des «*prescriptions . . . sur l'exercice du commerce et de l'industrie*». Cette disposition permet de restreindre les activités lucratives des particuliers par des mesures de police économique destinées à assurer la *loyauté en affaires*. Cette exigence de loyauté vaut également pour les traitements de données effectués en relation avec une activité économique, peu importe que le traitement constitue en soi cette activité économique – comme c'est le cas des centres de calcul – ou qu'il ne soit qu'un moyen à son service. Par contre, l'article 31^{bis}, 2^e alinéa, cst., n'est pas une base constitutionnelle adéquate permettant de réglementer les traitements de données effectués soit pour un usage exclusivement personnel, soit à des fins scientifiques ou idéales.

D'autres dispositions constitutionnelles viennent compléter ces deux normes fondamentales en habilitant la Confédération à légiférer sur la protection des données dans des domaines spécifiques. Ainsi, l'article 34^{ter}, 1^{er} alinéa, cst., permet de réglementer les systèmes d'informations relatifs au personnel en vue de protéger les travailleurs. De plus l'article 31^{quater} octroie à la Confédération la compétence de légiférer sur les systèmes d'informations des banques et des institutions de crédit; quant à l'article 34, 2^e alinéa, il l'autorise à régler les traitements de données effectués par des assurances privées.

122 Le droit public

Le législateur fédéral peut s'appuyer sur le *pouvoir d'organisation* que lui confère l'article 82, chiffre 1, cst., pour édicter des dispositions de protection des données applicables aux autorités et aux services administratifs. Cette norme constitutionnelle permet, d'une part, de déterminer à quelles conditions les services administratifs sont en droit de recourir à des traitements de données en tant qu'instrument de travail et d'organisation et d'autre part, d'instituer des instances de contrôle chargées d'assurer une protection des données efficace. De plus, la Confédération peut se fonder sur ses attributions générales en matière de droit pénal (art. 64^{bis} cst.) pour renforcer la protection pénale des données et, ce, soit en définissant de nouvelles infractions, soit en étendant le champ d'application du secret de fonction ou du secret professionnel.

La constitution reconnaissant aux *cantons* une pleine autonomie en matière d'organisation, il leur appartient de légiférer sur la protection des données dans leurs secteurs publics. Le droit cantonal détermine également dans quelle mesure la législation cantonale sur la protection des données est applicable aux communes. La Confédération n'est dès lors en droit d'édicter des dispositions de protection des données applicables aux secteurs publics cantonaux ou communaux que dans les domaines où les cantons sont chargés d'exécuter des prescriptions fédérales, prescriptions, il va sans dire, fondées sur une disposition constitutionnelle attributive de compétence. Un exemple: le domaine de la lutte contre les maladies transmissibles (art. 69 cst.). Reste que même dans ces cas la Confédération doit éviter d'empiéter sur les compétences cantonales en matière d'organisation.

13 Travaux préparatoires et procédure de consultation

131 Le droit général de la protection des données

La première motion tendant à l'adoption d'une loi sur la protection des données a été déposée par le conseiller national Bussey le 17 mars 1971. Le motionnaire souhaitait une législation «qui assure la protection du citoyen et de sa sphère privée contre l'utilisation abusive de l'ordinateur et qui permette d'autre part un développement normal de l'usage des ordinateurs»²²⁾. Cette motion a été transformée en postulat²³⁾. Le 22 mars 1977, le conseiller national Gerwig déposait à son tour deux initiatives parlementaires concernant la protection des données. La première initiative, qui se présentait sous la forme d'une proposition rédigée de toutes pièces, entendait doter la constitution d'un article sur la protection des données. Quant à la seconde initiative, qui, elle, n'était formulée qu'en termes généraux, elle énumérait les exigences que devrait remplir une loi sur la protection des données.

La commission du Conseil national chargée d'examiner les deux initiatives Gerwig ne s'était pas encore prononcée sur la suite à leur donner que le chef du Département fédéral de justice et police donnait mandat, en 1977, à un groupe d'experts de préparer une loi sur la protection des données, avec à la clé deux injonctions de principe. Première injonction: le projet de loi devra s'en tenir aux bases constitutionnelles actuelles et n'appréhender que le secteur privé et le secteur public fédéral; il était donc hors de question de modifier la constitution afin d'obtenir la compétence de légiférer dans le secteur public cantonal. Seconde injonction: les travaux relatifs au secteur privé et ceux relatifs au secteur public fédéral devront être menés séparément, tout au moins dans leur phase préliminaire.

Dans cette optique, une première commission fut chargée, en 1977, d'élaborer les dispositions de protection des données appelées à régir l'administration fédérale; placée sous la présidence du professeur Mario M. Pedrazzini de Saint-Gall, elle se composait de représentants des milieux de la science, de l'économie privée et de l'administration publique. Après avoir recensé les fichiers existants et dressé l'inventaire des problèmes soulevés par la protection des données, cette commission remit, en 1981, au chef du Département fédéral de justice et police un avant-projet de loi sur la protection des données dans l'administration fédérale. Entre-temps, le chef du Département fédéral de justice et police avait confié, en septembre 1979, à une deuxième commission d'experts, également présidée par le professeur Mario M. Pedrazzini, le soin d'établir des dispositions de protection des données applicables au secteur privé. Cette commission mena plusieurs enquêtes auprès d'une centaine d'entreprises, d'associations et d'organisations afin d'identifier les problèmes de protection des données qu'elles rencontrent et de déterminer dans quelle mesure elles ont recours à des fichiers. Elle acheva ses travaux en octobre 1982 en déposant un avant-projet de loi régissant le secteur privé.

En novembre 1982, le chef du Département fédéral de justice et police chargea un groupe de travail composé de membres des deux commissions de fondre les deux avant-projets de loi en un seul; au motif qu'il fallait d'une part éviter une

dispersion des normes qui s'avèrerait préjudiciable aux intérêts des personnes concernées et d'autre part simplifier le déroulement de la procédure législative. Le projet rédigé par ce groupe de travail fut *mis en consultation* à la fin de 1983.

Ce projet tentait de définir des critères permettant de pondérer deux intérêts divergents: d'un côté l'intérêt des organes étatiques et des particuliers à pouvoir disposer d'informations, de l'autre celui des personnes concernées à bénéficier d'une protection contre les traitements de données abusifs. A cet effet, et s'agissant du secteur privé, le projet instituait des règles différenciées sur le fardeau de la preuve d'une part au bénéfice des personnes concernées, d'autre part en faveur de certains traitements de données. En ce qui concerne le secteur public, le projet prévoyait des dispositions détaillées sur les traitements des données personnelles effectués par les organes fédéraux. En outre, il obligeait tant les organes de la Confédération que les personnes privées à faire enregistrer, dans certaines conditions, les fichiers qu'ils exploitent. Enfin, le projet accordait aux personnes concernées non seulement un droit d'accès, mais encore les moyens juridiques leur permettant de se défendre contre les atteintes à la personnalité causées par des traitements de données. On soulignera encore un point: une commission de protection des données était appelée à fonctionner comme organe de contrôle; si, pour le droit privé, cette commission était conçue sur le modèle de la Commission des cartels, ses attributions en droit public étaient comparables à celles du Contrôle fédéral des finances. Enfin, le projet prévoyait plusieurs dispositions pénales destinées à sanctionner la violation des principes fondamentaux de la protection des données.

132 La protection des données dans le domaine médical

En sus des règles générales sur la protection des données, il importe de prévoir des dispositions complémentaires valables pour certains domaines particuliers, tel que la médecine et les assurances sociales. Dans ces domaines en effet, le traitement de données sensibles est chose primordiale, même si parfois la sphère intime des personnes concernées en est atteinte. Par ailleurs, on ne saurait nier qu'il existe, du moins partiellement, un intérêt public prépondérant à l'exploitation de données sur la santé.

Soucieux de trouver une solution aux problèmes spécifiques que pose l'élaboration des normes de protection des données applicables au secteur médical, l'Office fédéral de la justice a réuni en 1980 une commission d'experts ad hoc, présidée par la conseillère nationale Yvette Jaggi, de Lausanne. Cette commission a publié son rapport en 1984; celui-ci inventorie les traitements de données caractéristiques du domaine médical et du domaine des assurances sociales, que ces traitements soient effectués par des personnes privées ou par des organes publics; après avoir passé en revue les bases légales de ces traitements, il analyse les divers problèmes de protection des données qu'ils soulèvent. Le rapport se conclut par un catalogue de recommandations; certaines d'entre elles sont concrétisées par le projet de loi qui vous est soumis; d'autres font toujours l'objet d'études approfondies au sein de l'administration.

En octobre 1983, le chef du Département fédéral de justice et police confiait à un autre groupe de travail, présidé par le professeur Günter Stratenwerth, de Bâle, le soin d'étudier les problèmes de protection des données inhérents à la recherche médicale. Ce groupe avait notamment pour mandat de trouver le juste équilibre entre l'intérêt des chercheurs à pouvoir traiter le plus grand nombre de données possible et l'intérêt des patients au respect du secret médical. A cette fin, il élaborait un catalogue de propositions, publié dans son rapport de décembre 1985. En substance, il parvient à la conclusion que des données personnelles soumises au secret médical ne peuvent être traitées à des fins de recherche scientifique qu'avec l'accord de la personne concernée. Sauf opposition expresse de la personne concernée, l'autorisation d'une commission d'experts ad hoc peut suppléer au défaut de consentement.

Se fondant sur ces travaux préparatoires, le Département fédéral de justice et police a préparé, en collaboration avec le Département fédéral de l'intérieur, un projet de loi sur la levée du secret professionnel en faveur de la recherche médicale. Ce projet a été mis en consultation au cours de l'été 1987. Il reprend pour l'essentiel les principes élaborés par le groupe de travail Stratenwerth. On relèvera que la portée de ce projet est limitée: il ne règlemente que l'un des aspects du traitement des données, *la communication*. A cette fin, il détermine à quelles conditions le secret de fonction peut être levé en faveur de la recherche médicale; dans cette perspective, il établit des normes d'application du secret médical institué par l'article 321 du code pénal. Soulignons enfin que le champ d'application du projet s'étend aux recherches conduites aussi bien par les services fédéraux que par les universités ou encore les hôpitaux cantonaux, régionaux ou communaux.

14 Les résultats de la procédure de consultation

141 La procédure de consultation concernant la loi sur la protection des données

Le projet de «loi fédérale sur la protection des données personnelles (LPD)» élaboré par la commission Pedrazzini a été mis en consultation le 25 janvier 1984. Six mois plus tard, 156 prises de position, dont certaines se révélèrent des plus étoffées, parvenaient au Département fédéral de justice et police. Des 141 organes officiellement invités à donner leur avis, 107 se sont prononcés, parmi eux l'ensemble des cantons. En outre, une cinquantaine d'organisations et de particuliers ont spontanément fait connaître leur point de vue.

En substance, la consultation a donné les résultats suivants: la grande majorité des organes consultés reconnaît la nécessité et l'urgence d'une législation sur la protection des données. Les dispositions du projet consacrées aux traitements de données effectués par l'administration fédérale ont été jugées satisfaisantes, voire bonnes; par contre, celles consacrées au secteur privé ont reçu un accueil défavorable. Du moins en règle générale; les syndicats, les corporations de droit public, les organisations scientifiques et culturelles, ainsi que les Eglises s'y sont ralliés; quant aux cantons, aux partis politiques et aux organisations professionnelles et féminines, ils ont émis, pour la plupart un jugement positif. Si l'avis

des informaticiens était partagé, celui des organisations économiques – à l'exception des organisations de consommateurs –, des associations patronales et des représentants des professions sociales était catégoriquement négatif. On relèvera en outre que le principe d'une loi commune au secteur public et au secteur privé a soulevé de vives controverses: certains cantons, partis politiques et organisations étaient pour, les autres cantons et les associations patronales contre.

Plusieurs propositions cardinales du projet ont été à l'évidence bien *acceptées*. Il en va ainsi de l'institution d'un régime juridique commun aux traitements de données automatisés et aux traitements de données manuels, de la création d'une catégorie spéciale de données, «les données sensibles», de l'obligation de faire enregistrer certains types de fichiers, et de l'octroi aux personnes concernées d'un droit d'accès et de rectification. Quant à la nécessité d'un contrôle efficace et indépendant, elle n'a pas été contestée, du moins dans son principe; il en va de même des dispositions pénales du projet de loi.

Reste que l'ampleur et la complexité du projet – il comptait 69 articles – ont été *critiquées*. En outre, certaines dispositions ont été jugées par trop abstraites, donc malaisées à mettre en œuvre. Autre source de difficultés: la réunion au sein d'un même article de règles valables les unes pour le seul secteur public, les autres pour le seul secteur privé. D'autre part, les présomptions et les fictions d'atteinte à la personnalité, de même que les motifs justificatifs, prévus pour le secteur privé, ont été jugés guère intelligibles. L'applicabilité de la loi aux autorités cantonales chargées d'exécuter le droit fédéral a également suscité des critiques. Certains organismes consultés ont souhaité que les personnes morales soient soumises à un régime juridique différent de celui des personnes physiques. Parmi eux les institutions d'évaluation du crédit, ces dernières craignant de voir leurs activités économiques par trop entravées. En outre, à plusieurs reprises, le vœu a été formulé que les dispositions spécifiques applicables aux médias, à la recherche et à la statistique, aux organes chargés de la sûreté de l'Etat et aux autorités fiscales soient réexaminées, soit pour être complétées, soit pour être précisées. Ajoutons enfin que l'institution d'une Commission de la protection des données fonctionnant comme organe de contrôle indépendant a recueilli les suffrages d'un grand nombre d'organismes consultés; cela dit, ceux qui se sont déclarés favorables à un préposé à la protection des données, sorte d'ombudsman de la protection des données, sont tout aussi nombreux.

142 La protection des données dans la recherche médicale

Le projet de «loi fédérale sur la levée du secret professionnel en faveur de la recherche médicale» a été mis en consultation le 27 mai 1987. A l'automne de cette même année, 54 prises de position parvenaient au Département fédéral de justice et police. Des 61 organismes officiellement invités à donner leur avis, 47 se sont prononcés; parmi eux, l'ensemble des cantons. En outre, sept organisations ont spontanément fait connaître leur point de vue.

Dans l'ensemble le projet fut bien accepté. La grande majorité des cantons, la quasi-totalité des Hautes-écoles, des organisations de médecins et de la recherche médicale ont en effet vu en lui une base adéquate pour une future loi. Si les avis

des partis politiques étaient partagés, les trois principaux se sont toutefois prononcés en faveur du projet. Par contre les organisations représentatives des intérêts des patients l'ont plutôt rejeté.

Mieux prendre en considération les droits des patients et mettre en évidence les aspects de protection des données fut le souhait de la majorité des organismes consultés. Une minorité mit en doute l'existence d'une base constitutionnelle permettant d'adopter sur le plan fédéral une réglementation de protection des données dans le domaine de la recherche médicale. En outre, des voix isolées se sont élevées contre la création d'une commission fédérale d'experts centralisant les autorisations et contre la fonction de contrôle attribuée au préposé à la protection des données dans le domaine de la recherche médicale.

Finalement plusieurs organismes consultés se sont prononcés en faveur d'une réglementation de ces questions dans la loi générale sur la protection des données et par une révision partielle du code pénal qui règle le secret professionnel.

15 La mise au point du projet

Début 1985, le Conseil fédéral prenait connaissance des résultats de la procédure de consultation relative à la loi sur la protection des données. Estimant qu'il était nécessaire de retravailler le projet en fonction de ces résultats, il confiait cette tâche à un groupe de travail restreint, présidé par le professeur Mario M. Pedrazzini. Ce groupe de travail élaborait un nouveau projet de loi; les représentants des associations patronales et des syndicats, des branches les plus importantes de l'économie – notamment les banques, les assurances, les marchands d'adresses et les médias –, ainsi que les offices fédéraux directement concernés eurent l'occasion de donner leur avis sur ce projet lors d'auditions organisées en mai 1986. Les organes consultés devaient saluer la nette séparation entre les dispositions applicables au secteur privé et celles applicables au secteur public. Ils se sont également plu à relever la plus grande concision et la meilleure lisibilité du projet. Quant au fond du projet, l'accueil fut plutôt mitigé: si certains organismes y ont souscrit sans réserve, d'autres ont formulé les mêmes critiques qu'à l'égard de l'avant-projet soumis en consultation en 1983. Suite aux auditions, le groupe de travail rédigea un nouveau texte qui fut remis au chef du Département fédéral de justice et police, en février 1987, accompagné d'un rapport explicatif.

Le chef du Département fédéral de justice et police chargea un groupe de travail interne à l'administration, présidé par Christoph Steinlin, docteur en droit et vice-directeur de l'Office fédéral de la justice, de revoir le projet sous l'angle de la systématique et de la rédaction afin de le simplifier et de le raccourcir substantiellement. Par la même occasion, les dispositions d'un projet de loi sur la levée du secret professionnel en faveur de la recherche médicale étaient intégrées à la loi sur la protection des données afin de réviser le code pénal. Signalons enfin que la procédure pénale fédérale et la loi sur l'entraide pénale internationale ont été complétées par des dispositions de protection des données applicables respectivement aux recherches préliminaires de la police judiciaire et aux échanges d'informations avec INTERPOL.

- 2** **Partie spéciale:**
Commentaire du projet de loi fédérale sur la protection des données, de la réglementation de la protection des données dans la recherche médicale et de la révision de la procédure pénale fédérale et de la loi sur l'entraide pénale internationale
- 21** **Les grandes lignes du projet de loi sur la protection des données**
- 211** **Une loi commune au secteur public et au secteur privé**

La procédure de consultation a révélé une forte opposition à une loi unique régissant à la fois le secteur privé et l'administration fédérale. Cette opposition était motivée par le fait que la protection des données dans l'administration fédérale et dans le secteur privé sont de conception fondamentalement différente; dès lors, une réglementation commune d'une part, serait difficilement réalisable et, d'autre part occasionnerait des complications d'ordre législatif. Le Conseil fédéral estime toutefois que le premier de ces arguments est dénué de tout fondement, le second par contre, tout en ne manquant pas de pertinence, ne justifie cependant pas à lui seul que l'on renonce définitivement aux avantages que procure une loi unique. Celle-ci a avant tout pour elle le fait que le but du législateur, à savoir la protection de la personnalité contre les atteintes imputables au traitement de données personnelles, est identique, que l'on se situe dans le secteur de l'administration fédérale ou dans le secteur privé. De surcroît, il est patent que les principes fondamentaux du droit de la protection des données s'appliquent aussi bien au secteur public qu'au secteur privé. Aussi est-il souhaitable que les mêmes autorités – c'est-à-dire le même préposé à la protection des données et la même Commission de la protection des données – se prononcent sur les questions de protection des données relevant des ces deux secteurs, encore qu'il faille admettre que, s'agissant du secteur privé, les compétences de ces deux organes doivent être bien moindres. Ce n'est qu'en réglant dans une même loi les problèmes inhérents à ces deux secteurs que l'on pourra garantir au mieux le développement harmonieux et coordonné de la protection des données en droit public et en droit privé. Une loi unique se justifie d'ailleurs d'autant plus que le projet sépare distinctement le secteur public du secteur privé. En outre, il stipule clairement que la réglementation applicable au secteur privé s'inscrit dans le cadre des règles générales sur la protection de la personnalité posées par le code civil. Dernier argument: seule une loi unique permet d'éviter les redondances et de contenir le nombre des normes dans les limites du strict nécessaire.

212 Champ d'application

Tout législateur qui entend s'attaquer à une loi générale sur la protection des données se voit nécessairement confronté à deux difficultés majeures. Le droit de la protection des données a un caractère global; à l'ère de l'informatique, en effet, presque aucune activité publique ou privée ne lui échappe. Vu le grand nombre de moyens techniques dont on dispose aujourd'hui, le traitement des données, qui est

l'objet même d'une loi sur la protection des données, prend les formes les plus diverses. Il est cependant impossible au législateur de prendre en compte chacune de ces différentes formes; il doit plutôt poser les principes généraux permettant d'esquisser une solution pour la plupart des problèmes tout en réservant l'avenir. En conséquence, le projet ne peut pas d'emblée réglementer spécifiquement l'ensemble des secteurs.

Il s'ensuit que le projet, à l'instar de nombre de lois étrangères²⁴⁾, n'établit pas de distinction entre les traitements de données manuels et les traitements automatisés. Refusant de se fonder sur des notions techniques précises, il demeure neutre face au développement de la technique. Autre conséquence du caractère général de la loi: celle-ci s'applique à toutes les données sans exception. Nous avons en effet délibérément renoncé à créer une catégorie de données dites «librement disponibles» – autrement dit une catégorie de données échappant au champ d'application de la présente loi –, d'abord parce qu'une telle catégorie est difficile à cerner, ensuite parce que toute information est susceptible, si le contexte s'y prête, de donner lieu à une atteinte à la personnalité. La loi entend en outre protéger aussi bien la *personne physique* que la *personne morale*, étant donné que l'une comme l'autre peut être atteinte dans ses droits. En contrepartie, les prescriptions sur le traitement des informations doivent être identiques. Polyvalente, la loi l'est également par le fait qu'elle régit aussi bien le secteur privé que le secteur public.

Le champ d'application de la loi sur la protection des données a toutefois ses *limites*. Il ne s'étend en effet pas aux procédures juridictionnelles devant les autorités judiciaires, aux procédures pénales, aux procédures d'entraide judiciaire, ni aux registres publics. Pourquoi? Les lois de procédure protègent déjà la personnalité; dès lors, il n'y a pas lieu de les doubler par des dispositions relevant du droit de la protection des données, d'autant que ce droit est en lui-même, partiellement du moins, du droit de procédure. Au demeurant, les travaux préparatoires au présent projet de loi ont démontré la nécessité de compléter les dispositions sur l'*enquête préliminaire* contenue dans la loi fédérale sur la procédure pénale par des garanties de protection des données. En conséquence, nous proposons, en annexe au présent projet, d'insérer dans la procédure pénale fédérale des dispositions garantissant la protection des données. Dans la foulée, nous proposons également de modifier la loi fédérale sur l'entraide pénale internationale: il importe d'une part de donner une base légale aux échanges de données dans le cadre de l'Organisation internationale de police criminelle (INTERPOL), et d'autre part de réglementer spécifiquement la protection des données dans ce domaine.

Le projet mis en consultation en 1983 prévoyait que la loi fédérale sur la protection des données était, exceptionnellement, applicable aux cantons dépourvus de législation suffisante sur la protection des données, lorsqu'ils exécutaient des lois fédérales. Cette extension du champ d'application prétendait d'un côté harmoniser le droit suisse de la protection des données et de l'autre empêcher la création de «paradis de données». Le projet qui vous est soumis renonce à aller aussi loin: il n'aurait guère été aisé de déterminer dans quelle mesure une loi cantonale offre des garanties «suffisantes», d'autant que l'on se doit d'interpréter les normes cantonales avec retenue. D'un côté, la Confédération ne pourrait pas

se satisfaire de la simple existence d'une loi cantonale sans risquer des solutions inéquitables; de l'autre, si elle n'entendait pas se contenter d'accepter les législations cantonales sur la protection des données sans examen approfondi, elle ne pourrait qu'instituer une procédure d'approbation; sans compter, pour le cas où le droit cantonal serait jugé insuffisant, l'imposition de normes fédérales supplétives. Il se pourrait alors que dans un même canton la protection des données relève de deux régimes juridiques différents selon que les lois exécutées sont cantonales ou fédérales. Dès lors, le Conseil fédéral estime qu'il n'y a pas lieu d'étendre le champ d'application de la loi fédérale sur la protection des données aux cas d'exécution par les cantons des lois fédérales.

213 Loi fédérale générale sur la protection des données

213.1 Principes matériels et organisationnels de la protection des données

Les *dispositions générales* de la première section renferment les principes directeurs indispensables à une protection des données vraiment efficace. Ces principes régissent aussi bien ceux qui traitent des données à titre privé que les organes de la Confédération. Ainsi, l'article 4 stipule que des données personnelles ne peuvent être collectées que par des *procédés licites et conformes à la bonne foi*. En outre, les données traitées doivent être *exactes*. Quant au traitement, il doit être conforme au *principe de la proportionnalité*. De surcroît, il est interdit, sauf disposition légale contraire, de *traiter des données dans un but autre* que celui qui a été indiqué lors de leur collecte ou qui ressort des circonstances. Enfin, toute personne qui traite des données a l'obligation d'*empêcher*, au moyen de mesures d'organisation et de mesures techniques appropriées, la *main-mise de tiers* sur les données. Ajoutés au principe gouvernant la communication des données à l'étranger (cf. ch. 213.5), ces principes forment le *noyau dur* de la protection des données.

Encore faut-il que les principes qui viennent d'être énoncés trouvent leur concrétisation dans la réalité; à cet effet, il importe d'instituer le cadre organisationnel et procédural nécessaire. Il s'agit de faire en sorte que la personne concernée soit à même de se rendre compte, dans une certaine mesure, que ses données font l'objet d'un traitement. Dans cette optique, les maîtres de fichiers sont tenus de *renseigner toute personne qui en ferait la demande sur les données la concernant qui sont contenues dans le fichier et sur la gestion de ce même fichier*. Du moment que seul celui qui connaît l'existence d'un fichier peut exercer son *droit d'accès*, il importe que tous les services fédéraux soient obligés de faire enregistrer leurs fichiers auprès du préposé à la protection des données. Les personnes privées sont soumises à une obligation d'enregistrer moins étendue; elles ne doivent annoncer un fichier que s'il y a un risque sérieux d'atteinte à la personnalité. Enfin, il y a également lieu, sous certaines conditions, de déclarer les communications de données à l'étranger (cf. ch. 213.5).

213.2 Protection des données dans le domaine du droit privé

La deuxième section du présent projet ne compte que quatre articles; elle renferme les prescriptions régissant les traitements de données effectués par des personnes physiques ou morales, soumises au droit privé. Une première proposition tendant à réglementer ce domaine fut discutée lors des travaux préparatoires à la nouvelle du 16 décembre 1983, révisant les articles 28 du code civil et 49 du code des obligations; cette proposition devait par la suite être retirée et renvoyée à examen plus approfondi dans le cadre de la législation sur la protection des données. Ainsi, dans sa partie consacrée au droit privé, le droit de la protection des données complète et concrétise les règles sur la protection de la personnalité instituées par le code civil. Aussi, le présent projet se conforme-t-il à la terminologie et à la systématique du code civil. La loi est censée fournir à ceux qui traitent des données, comme aux juges, les éléments leur permettant d'apprécier dans quels cas un traitement de données est susceptible de porter une atteinte illicite à la personnalité d'une personne. Certaines activités, notamment celles qui transgressent les principes généraux applicables au traitement, sont considérées, de par la loi, comme portant illicitement atteinte à la personnalité. D'un autre côté, le projet indique également quelles circonstances peuvent justifier une atteinte à la personnalité. C'est ainsi que l'on ne saurait oublier que la concurrence économique présuppose d'intenses collectes et traitements de données. De même, il peut arriver, dans certains cas, que la nécessité d'obtenir des informations sur un concurrent, sur un cocontractant ou sur une personne dont on veut évaluer le crédit, légitimise une atteinte à la personnalité de la personne concernée. Partant, le jeu complexe – et très critiqué lors de la procédure de consultation – des fictions et des présomptions a été abandonné au profit d'un système plus flexible, permettant de tenir compte des particularités de chaque cas d'espèce. Enfin, pour ce qui concerne la protection juridique, le projet renvoie pour l'essentiel aux articles 28 à 28f du code civil.

213.3 La protection des données dans le secteur public

La section du projet consacrée au secteur public régit les traitements de données effectués par l'administration fédérale ainsi que par des particuliers ou des organisations chargés d'exécuter des tâches publiques. Elle part de l'idée que tout traitement de données personnelles entrepris par l'administration peut porter atteinte – plus ou moins fortement il est vrai – aux droits fondamentaux des personnes concernées. C'est pourquoi, il importe que la future loi sur la protection des données garantisse que ces traitements respectent les principes de légalité et de proportionnalité. En conséquence, les organes fédéraux ne seront en droit de traiter des données personnelles que s'il existe une base juridique à cet effet. Des conditions plus sévères – quant à l'exigence d'une base légale, d'une autorisation du Conseil fédéral ou du consentement de la personne concernée – seront mises au traitement de données sensibles ou à l'établissement de profils de la personnalité. En outre, certaines formes particulières de traitement, notamment la collecte, la communication, l'anonymisation et la destruction des données, feront l'objet des *dispositions spéciales*. La statistique, la recherche et la planifica-

tion bénéficieront d'un régime juridique moins sévère du moment que le but du traitement ne se rapporte pas à des personnes. Enfin, le Conseil fédéral se voit octroyer la compétence d'édicter, pour les domaines de la protection de l'Etat et de la sécurité militaire, des dispositions relatives au traitement qui dérogent aux principes de la loi. Celle-ci renferme en outre des dispositions de procédure. Certaines d'entre elles tendent à clarifier des règles déjà existantes, d'autres apportent des innovations, telle la possibilité de faire porter la mention du caractère litigieux d'une donnée que la personne concernée a mis en doute.

213.4 Dispositions pénales et organisationnelles

Le présent projet institue un préposé fédéral à la protection des données et une Commission fédérale de la protection des données, chargés de veiller au respect de la loi.

Le *préposé à la protection des données* jouera avant tout le rôle de médiateur entre ceux qui traitent les données et les personnes concernées. Si un traitement de données est controversé, il peut ouvrir une enquête; il s'ensuit que ses compétences de contrôle sur le secteur public sont très étendues. Il n'en va pas de même dans le secteur privé: là, il appartient avant tout au juge civil de se prononcer sur les prétentions de la personne concernée découlant du droit de la protection des données. Le préposé à la protection des données n'est en droit d'intervenir que si les méthodes de traitement utilisées font courir à un grand nombre de personnes un risque sérieux d'atteinte à la personnalité. Le préposé n'est pas juridiquement en droit d'exiger des organes et des particuliers de mettre fin aux irrégularités; il doit se limiter à faire des recommandations. Reste que si ces recommandations ne sont pas suivies, il peut porter l'affaire devant la Commission fédérale de la protection des données pour décision.

La *Commission fédérale de la protection des données* disposera, dans le secteur public, de larges prérogatives; en revanche, s'agissant du secteur privé, la commission ne sera en mesure de s'en prendre qu'aux traitements de données qui présentent un risque sérieux pour un grand nombre de personnes. Elle se prononce en première instance sur les recommandations du préposé à la protection des données; de plus, elle examine les recours d'une part contre les décisions des organes fédéraux en matière de protection des données, d'autre part contre les décisions cantonales de dernière instance, prises en application des dispositions de droit public fédéral. Les décisions de la Commission de la protection des données peuvent être portées devant le Tribunal fédéral.

La réglementation sur la protection des données instituée par la loi est renforcée par des *dispositions pénales*. Ainsi, celui qui collecte illicitement des données personnelles est punissable; il en va de même de celui qui communique des données personnelles secrètes dont il a eu connaissance dans le cadre de ses activités professionnelles. Enfin, sont également sanctionnables pénalement la personne privée, maître de fichier, qui ne respecte pas le droit d'accès de la personne concernée ou qui contrevient à son obligation de déclarer un fichier, ainsi que la personne privée qui refuse de collaborer à une enquête menée par le préposé à la protection des données.

213.5 La protection transfrontière des données

L'échange de données entre la Suisse et l'étranger doit être réglé spécifiquement, et ce, contrairement à ce qui vaut pour le flux d'informations entre l'administration fédérale et les cantons. Le droit de la protection des données ne peut pas ignorer l'importance considérable des flux transfrontières d'informations. S'il est déjà difficile d'offrir, en droit interne, à la personne concernée la protection qu'elle attend, il l'est d'autant plus s'agissant des traitements de données transfrontières. Dans ce domaine plus qu'ailleurs, une intervention du législateur s'impose. Reste que la réglementation spécifique nécessaire ne doit en principe pas entraver la circulation internationale des informations.

La réglementation des flux transfrontières de données prévue par le présent projet s'articule autour de trois principes. Premièrement, ni les organes publics, ni les personnes qui traitent des données à titre privé ne sont en droit de communiquer des informations à l'étranger, si le traitement menace la personnalité des personnes concernées. Tel peut être le cas, si des données délicates sont transmises à un Etat dépourvu d'une législation sur la protection des données comparable à la législation suisse. Deuxièmement, les organes fédéraux sont tenus de se soumettre aux règles générales sur la communication lorsqu'ils transmettent des données à l'étranger. Il s'ensuit principalement qu'ils ne peuvent communiquer des données à l'étranger que s'il existe une base juridique à cet effet ou si le destinataire des données en a besoin pour accomplir sa tâche légale. Troisièmement, il incombe aux personnes privées comme aux organes fédéraux qui entendent communiquer des données à l'étranger, régulièrement ou en grand nombre et à l'insu de la personne concernée, d'en informer le préposé à la protection des données; au besoin, celui-ci attirera leur attention sur les dangers qu'ils font courir aux personnes concernées.

214 Protection des données dans la recherche médicale

Le consentement de la personne concernée n'est pas l'unique moyen de lever le secret professionnel à des fins de recherche médicale; celui-ci peut être aussi levé par le biais d'une autorisation d'une commission d'experts nommée par le Conseil fédéral. Toutefois cette dernière n'octroiera l'autorisation qu'aux conditions suivantes: la recherche ne peut être effectuée avec des données anonymes et il est particulièrement difficile d'obtenir le consentement de l'intéressé. Au demeurant les intérêts de la recherche priment les intérêts des personnes concernées, en particulier des patients, au maintien du secret. Ainsi, le projet de recherche doit répondre à de hautes exigences qualitatives pour justifier la levée du secret professionnel. Dans certains cas cependant, la procédure d'autorisation pourra être simplifiée. C'est ainsi que la Commission d'experts sera en mesure d'octroyer une autorisation générale à une clinique ou à un institut, notamment pour la recherche interne, pour l'élaboration de thèses de doctorat ou pour la gestion de registres médicaux. De telles simplifications ne sont toutefois possibles que si les intérêts de la personne concernée sont préservés et les données personnelles sont d'emblée rendues anonymes. Indépendamment de toute procédure, la personne concernée peut toujours s'opposer à la communication de ses données.

La Commission est une autorité fédérale indépendante. Elle se fait conseiller par le préposé fédéral à la protection des données. Ce dernier contrôle en outre l'octroi des autorisations. Il peut porter les décisions de la Commission d'experts devant la Commission fédérale de la protection des données.

La levée du secret professionnel en faveur de la recherche médicale nécessite avant tout une modification du code pénal (art. 321 CP). Ainsi la protection des données dans ce domaine sera régie par le code pénal et la loi sur la protection des données. Tenant compte des résultats de la procédure de consultation, on a renoncé à élaborer une loi spécifique.

215 Révision de la loi sur la procédure pénale fédérale et de l'entraide judiciaire

La procédure pénale fédérale échappe à la loi sur la protection des données. Cette restriction du champ d'application crée une lacune: aucun principe de protection des données ne régit les recherches préliminaires entreprises par la police judiciaire. Cette lacune, nous proposons de la combler par une révision de la loi sur la procédure pénale fédérale. Il importe de trouver un juste équilibre entre deux intérêts apparemment contradictoires: d'un côté celui de la police judiciaire à pouvoir poursuivre les infractions, de l'autre celui des personnes concernées à sauvegarder leur sphère privée. Ainsi, par égard pour la liberté d'expression, la police judiciaire ne sera désormais en droit de *filmer ou de photographier une manifestation publique* qu'à certaines conditions: il faudra qu'il ressorte effectivement des circonstances que les manifestants envisagent de commettre un crime ou un délit dont la gravité ou la particularité justifie cette mesure. En outre, la réglementation proposée fait bénéficier la personne concernée d'un *droit d'accès et de rectification* des données contenues dans les dossiers de la police judiciaire; il est également prévu de réglementer la communication de ces données à d'autres autorités publiques. La personne concernée qui se voit refuser l'accès à ses propres données peut saisir le préposé à la protection des données; celui-ci peut alors faire des recommandations au responsable de la police judiciaire, le procureur général de la Confédération. Si ce dernier et le préposé n'arrivent pas à s'entendre, ils peuvent porter l'affaire devant la Chambre d'accusation du Tribunal fédéral. Semblable solution existe déjà en matière d'écoutes téléphoniques.

Enfin, nous proposons de créer une base légale pour la fouille, l'examen médical et les mesures d'identification. Ces mesures ne relèvent pas de la protection des données au sens strict; toutefois leur réglementation s'impose, car elles peuvent porter à la personnalité des personnes concernées une atteinte aussi grave que les traitements de données personnelles.

Par la même occasion, nous proposons de créer aussi une base légale pour les échanges d'informations entre le Ministère public de la Confédération et l'Organisation internationale de police criminelle INTERPOL. La protection des données dans ce domaine est avant tout régie par les statuts et règlements d'INTERPOL, pour autant que le Conseil fédéral les ait déclarés applicables. Quant au préposé à la protection des données, s'il est en droit de conseiller les services administratifs, il ne peut en revanche porter une affaire devant la

Commission de la protection des données. Cette limitation ne vaut pas pour les données de nature non criminelle, tels les signalements des personnes disparues ou d'inconnus. Dans ces cas, le préposé peut exercer l'ensemble des prérogatives que lui octroie la loi générale sur la protection des données.

22 Commentaire du projet

221 La loi sur la protection des données

221.1 Section 1: But, champ d'application et définition

Article premier But

L'article premier du projet rappelle les fondements du droit de la protection des données: la protection de la personnalité, s'agissant des échanges d'informations entre privés, les droits constitutionnels, en particulier le droit constitutionnel non écrit à la liberté personnelle, s'agissant des traitements de données effectués par des autorités publiques. Le but de la protection des données est, d'une part, de préciser le contenu de ces biens juridiques que sont la personnalité et la liberté personnelle lors des traitements d'informations et, d'autre part, de les défendre contre certains traitements de données. L'article premier est ainsi censé maintenir l'interprétation des diverses dispositions de la loi dans le sillage de la protection de la personnalité et des droits fondamentaux.

La loi fait bénéficier tant les *personnes physiques* que les *personnes morales* des prétentions qui découlent de la protection des données. Suivant les règles sur le droit de la personnalité posées par le code civil, le cercle des personnes morales s'étend non seulement aux personnes morales du droit privé et du droit public, fédéral et cantonal, mais aussi aux personnes morales du droit public étranger, pour autant que la capacité civile leur soit reconnue. Ne sont en revanche pas protégés – ce qui est également en concordance avec le droit de la personnalité –, les groupements de personnes auxquels le droit suisse dénie la personnalité juridique. Cela dit, la loi étend sa protection aux sociétés de personnes qui, bien que ne jouissant pas de la personnalité morale, bénéficient de la capacité juridique; tel est le cas des sociétés en commandite et des sociétés en nom collectif. Par contre ne sont pas couverts les groupements de personnes qui, d'après le droit suisse, ne possèdent pas la capacité juridique, tels les groupes ethniques ou les sociétés simples. Certes, on pourrait se demander si ces groupes de personnes, étant donné les atteintes dont elles pourraient être victimes, ne devraient pas également bénéficier de la protection de la loi. La réponse doit cependant être négative: il n'appartient pas à la loi sur la protection des données, dont la partie afférent au droit privé est conçue comme un complément au code civil, de créer de nouvelles catégories de personnes morales. Dès lors, chaque membre de ces groupes de personnes est renvoyé à faire valoir en son propre nom les prétentions qui découlent de la protection des données.

Deux questions ont été particulièrement débattues lors des travaux préparatoires au projet, et notamment lors de la procédure de consultation: premièrement faut-il, s'agissant du domaine du droit privé, faire bénéficier les personnes morales de la même protection que les personnes physiques? Deuxièmement, les per-

sonnes morales peuvent-elles faire valoir des prétentions découlant de la partie consacrée au droit public de la loi, partie qui est censée concrétiser les droits fondamentaux. Selon certains, la loi ne devrait accorder aucune protection aux personnes morales (à l'instar des lois allemande et française notamment) ou, tout au plus, une protection très atténuée, puisque ces personnes exerçant des activités économiques doivent faire preuve d'une certaine transparence, notamment dans l'intérêt des créanciers. C'est un fait que, contrairement à de simples particuliers, les personnes et les entreprises économiques qui affrontent la concurrence non seulement suscitent l'intérêt du public mais encore font l'objet d'une surveillance étroite de la part de leurs concurrents. S'agissant des corporations de droit public ou des établissements, un intérêt public prépondérant peut justifier de rendre publiques leurs activités. Dans cette optique, il peut être opportun de ne pas accorder aux personnes morales tous les moyens juridiques qu'offre la protection des données. Une exclusion – même partielle – des personnes morales du champ de protection de la présente loi romprait avec la tradition juridique suisse. L'article 53 du code civil ne protège-t-il pas justement les personnes morales contre les traitements d'informations illicites, notamment les atteintes portées à leur honneur ou – ce qui est tout particulièrement important dans la concurrence économique – à leur sphère privée²⁵⁾? Au demeurant, une discrimination des personnes morales aurait dans les faits des conséquences néfastes. Celle-ci serait d'autant plus choquante que, dans les petites entreprises, les informations sur les personnes morales sont souvent en relation étroite avec les personnes physiques. Ainsi, les personnes morales à but non économique tels les partis politiques, les organisations caritatives et les églises devraient se passer de protection des données. De l'autre côté, il est impossible d'exclure du champ de protection de la loi les seules personnes morales qui exercent une activité économique sans que cela ait pour conséquence de *privilégier les personnes physiques* avec qui elles sont en concurrence. C'est la raison pour laquelle nous estimons que la présente loi doit, en ce qui concerne le secteur privé, accorder une *protection identique* aux personnes physiques et aux personnes morales. Il importe également d'accorder aux personnes morales une protection pleine et entière à l'encontre des traitements de données effectués par des autorités publiques; et ce, alors même que la doctrine dominante soutient que les personnes morales ne peuvent invoquer les droits fondamentaux pertinents en matière de protection des données, notamment la liberté personnelle²⁶⁾. On ne saurait en effet nier que les personnes physiques et les personnes morales ont, en matière de protection des données, des exigences très semblables; dès lors, une personne morale est en droit de se prévaloir de la liberté personnelle à l'encontre de certains traitements de données. Il serait d'autant moins justifié de discriminer les personnes morales, s'agissant du secteur public, que celles-ci peuvent incontestablement invoquer, en matière de protection des données, les principes généraux du droit public que sont le principe de l'égalité et celui de proportionnalité.

En revanche, le projet de loi ne s'applique pas aux organisations internationales. Celles-ci, en tant que sujets du droit international public, ne peuvent pas sans autre être soumises au droit étatique. La réglementation de protection des données dans le cas des organisations internationales devra dès lors figurer dans les accords de siège. Cela vaut aussi pour le Comité international de la Croix-

rouge (CICR). Bien que le CICR soit une association régie par le code civil suisse, la doctrine le considère de plus en plus comme un sujet du droit international et l'assimile à une organisation internationale²⁷). Cette évolution ne peut être ignorée de la législation sur la protection des données. Le CICR ne peut en effet remplir ses tâches de manière efficiente s'il est contrôlé par une autorité étatique, en particulier par un préposé à la protection des données au sens du présent projet. Par ailleurs, l'agence centrale de recherches du CICR est déjà soumise à une réglementation interne très stricte en matière de protection des données.

Article 2 Champ d'application

Selon le 1^{er} alinéa, la loi impose des obligations et aux personnes dites privées et aux organes fédéraux. L'expression *personne privée* (let. a) désigne les personnes qui traitent des données dans le cadre d'une relation de droit privé. La catégorie des *organes fédéraux* (let. b) comprend en premier lieu toutes les unités administratives de la Confédération qui œuvrent de manière indépendante dans une sphère d'attribution précise. Cette définition vise également toutes les personnes *physiques et morales* qui exécutent des tâches publiques pour le compte de la Confédération (cf. art. 3, let. c et d, et notre commentaire à ce sujet).

Il ne sera par toujours aisé de déterminer si celui qui traite les données doit être qualifié de personne privée ou d'organe public. Un critère décisif sera la nature juridique de l'activité occasionnant le traitement: l'activité ressortit-elle au droit privé ou au droit public? Ainsi seront, entre autres, considérés comme des organes publics, les établissements autonomes qui œuvrent dans le domaine de l'assurance-vieillesse et survivants et de l'assurance-chômage – à commencer par la CNA et les caisses de compensation privées, et ce, parce que leurs activités sont en grande partie réglées par le droit administratif fédéral. Il est en revanche beaucoup plus difficile de se prononcer sur les caisses-maladie. Celles-ci doivent être considérées comme exécutant des tâches publiques fédérales et, partant, soumises aux prescriptions de la loi applicables aux organes fédéraux, si elles sont reconnues par la Confédération, si elles disposent des prérogatives des puissances publiques et si leurs activités sont régies par la loi sur l'assurance-maladie. La distinction n'est pas dénuée d'importance, car les organes publics sont soumis à des règles de protection des données plus sévères et plus circonstanciées que les personnes privées.

Le 2^e alinéa prévoit différentes limites du champ d'application:

Lettre a Traitement pour un usage exclusivement personnel

Tant les obligations légales qui incombent aux personnes qui traitent des données que les droits des personnes concernées ne sont pas sans limites: les uns et les autres s'arrêtent au seuil du domaine personnel, au sens strict, de la personne qui traite des données. Il ne serait guère raisonnable d'appliquer la loi sur la protection des données aux personnes physiques qui traitent des données pour un *usage exclusivement personnel*. Que l'usage à titre privé d'une donnée échappe au droit n'est pas nouveau: il suffit de se reporter à la législation sur le droit d'auteur pour trouver un précédent²⁸). L'expression «usage exclusivement personnel» vise surtout la famille et les proches. Ainsi, il est hors de question de contraindre un particulier à révéler le contenu de son agenda. De même, les conversations au sein

du cercle familial ou des amis et la correspondance privée ne tombent pas sous le coup de la loi sur la protection des données. Ne tombent pas non plus sous le coup de cette loi les notes que tout un chacun est amené à prendre dans l'exercice de sa profession à titre de pense-bête, du moment qu'il n'en fait qu'un usage personnel. Cela dit, si un traitement de données à un usage exclusivement personnel vient néanmoins à porter atteinte à la personnalité – par exemple une lettre égarée dont un tiers prend connaissance –, la victime n'est pas dépourvue de tout moyen juridique: elle peut toujours faire valoir les prétentions qui découlent de la protection générale de la personnalité instituée par l'article 28 du code civil. Au reste, il appartient à la jurisprudence de veiller à ce que celui qui traite les données ne se retranche pas abusivement derrière l'exception instituée par l'article 2, 2^e alinéa, lettre a, notamment pour échapper aux obligations qui lui incombent en vertu du droit d'accès.

Lettre b L'exception en faveur des médias

La novelle du 16 décembre 1983 modifiant l'article 28 du code civil a contribué de façon essentielle à renforcer la protection de la personnalité face aux médias. Se fondant sur les articles 28g et suivants du code civil, la personne concernée peut exercer un droit de réponse à l'encontre d'informations parues dans les médias à caractère périodique, telle la presse, la radio ou la télévision. Ce moyen de défense spécifiquement adapté aux particularités des atteintes à la personnalité par des médias se suffit à lui-même: il n'a donc pas besoin d'être complété par des prescriptions de protection des données. Ainsi, le projet laisse-t-il ce domaine de côté. En revanche, la loi sera applicable aux médias à caractère périodique tant que les données *n'ont pas encore été publiées*. Cela dit, la loi prévoit des allègements pour la phase précédant la publication (cf. art. 10, 2^e al., let. d).

Lettre c L'Assemblée fédérale

La loi ne régit pas *les affaires du ressort de l'Assemblée fédérale*. Le parlement ne serait pas en mesure d'exercer ses attributions constitutionnelles de haute surveillance sur l'administration et les tribunaux (art. 85, ch. 11, cst.), s'il était tenu de se conformer dans tous les cas aux principes fondamentaux de la protection des données, en particulier aux restrictions mises à la communication de données personnelles. Au surplus, les débats des chambres fédérales sont, de par la constitution (art. 94 cst.), publics. Enfin, la loi sur le rapport entre les conseils, les règlements des deux chambres, ainsi que ceux des commissions, contiennent des règles relativement circonstanciées sur le traitement des informations dans les procédures parlementaires²⁹). Ainsi, les commissions de gestion des chambres fédérales sont, sur la base de l'article 47^{quater} de la loi sur les rapports entre les conseils (RS 171.11), en droit de demander des renseignements utiles à toutes les autorités et à tous les services, et ce indépendamment du secret de fonction. Toutefois le Conseil fédéral peut présenter un rapport spécial au lieu de produire des documents lorsqu'il importe de sauvegarder des intérêts dignes d'être protégés. L'applicabilité de la loi sur la protection des données à ce domaine ne manquerait pas de faire problème: il ne serait souvent guère aisé de déterminer lequel de ces textes trouve application. L'exception vise non seulement les activités parlementaires au sens strict, mais aussi les Services du parlement, pour autant que leurs activités soient directement au service du parlement. Tel n'est pas

le cas, par exemple, de la gestion des dossiers du personnel de ces services, qui, elle, reste dès lors soumise à la loi.

Contrairement au projet de 1983, le champ d'application de la loi s'étend aux *activités gouvernementales du Conseil fédéral*. Le Conseil fédéral devra donc respecter les principes posés par celle-ci. Au demeurant, les délibérations du Conseil fédéral resteront secrètes comme par le passé; il en va de leur objectivité. A lui seul, ce motif ne saurait justifier une exclusion du Conseil fédéral du champ d'application de la loi sur la protection des données: l'article 13 de la loi sur l'organisation de l'administration dispose déjà que les délibérations du Conseil fédéral ne sont pas publiques. Cette disposition, à l'instar de celles concernant le huis clos des tribunaux, prive la personne concernée de tout droit d'accès aux délibérations du Conseil fédéral. En tant que norme spéciale, elle prime la loi sur la protection des données. Nous avons affaire là à une restriction légale du droit d'accès au sens de l'article 6 du présent projet. Au reste, l'article 24, 1^{er} alinéa, prévoit que le Conseil fédéral échappe à la surveillance du préposé à la protection des données.

Lettre d Procédure juridictionnelle

Les procédures juridictionnelles suivent des règles précises contenues dans les lois de procédure. Le but de ces normes est de protéger la personnalité des personnes impliquées dans la procédure. C'est le cas notamment des dispositions sur le droit d'être entendu, le droit d'accéder aux dossiers et le droit de participer à l'administration des preuves. Les lois de procédure renferment également des dispositions topiques sur le traitement de l'information: celles-ci déterminent de quelle manière le dossier doit être constitué et apprécié. Les lois de procédure pondèrent aussi l'intérêt du juge et des parties à obtenir une information et l'intérêt au maintien du secret qu'a une personne appelée à témoigner; tel est le cas, par exemple, des règles sur le refus de témoigner. En ce sens, le droit de procédure peut être considéré comme du droit de la protection des données. Si la loi sur la protection des données venait à s'appliquer aux procédures juridictionnelles, on se trouverait en présence de deux législations visant, partiellement du moins, un seul et même but. Cette dualité pourrait menacer la sécurité juridique, causer des problèmes de coordination et, finalement, retarder inutilement la procédure. Ces conséquences néfastes, l'exception instituée par la lettre d tend à les éviter.

C'est ainsi que la loi ne s'applique pas non plus aux procédures devant le Tribunal fédéral et devant les commissions fédérales de recours ou d'arbitrage; peu importe qu'il s'agisse de procédures en première instance ou de procédures de recours. Cette exception ne vaut cependant que pour les procédures *pendantes*. De ce fait, la loi régit tout traitement de données postérieur à la clôture de la procédure, notamment la conservation et la destruction des pièces de procédure, ou leur communication à des tiers. De même, les traitements de données effectués par les *services administratifs des tribunaux* (p. ex. les greffes) sont soumis à la loi.

Lettre e Les procédures pénales

L'exception relative aux procédures pénales répond aux mêmes motifs que celle concernant les procédures juridictionnelles devant les autorités judiciaires (let. d).

Par procédure pénale, il faut entendre les causes relevant de la procédure pénale fédérale, de la procédure pénale administrative et de la procédure pénale militaire. Si nous avons dû créer une disposition spéciale pour ces procédures, c'est parce que les lois sur la procédure pénale fédérale et la procédure pénale militaire renferment également des dispositions sur les recherches préliminaires, lesquelles n'ont pas un caractère juridictionnel, mais administratif: en effet, d'une part, le procureur général de la Confédération qui dirige les recherches de la police judiciaire, est un organe juridictionnel, d'autre part, le Ministère public fait partie de l'administration fédérale. Enfin, l'exception vise également les autorisations données par le Département fédéral de justice et police à l'ouverture d'une poursuite pénale contre un fonctionnaire au terme de l'article 15 de la loi fédérale sur la responsabilité (RS 170.32).

Lettre f Les procédures d'entraide judiciaire internationale concernant des causes civiles ou pénales

La loi sur la protection des données ne s'applique en outre pas aux procédures d'entraide judiciaire internationale concernant les causes civiles ou pénales. D'abord une demande d'entraide découle toujours d'une procédure, pénale ou civile; ensuite la loi sur l'entraide judiciaire contient déjà certaines dispositions tendant à protéger la personnalité (cf. ch. 224). De surcroît, l'entraide judiciaire en matière civile ressortit principalement aux tribunaux cantonaux; dans ce domaine, la Confédération (Office fédéral de la police) n'est qu'une courroie de transmission.

Lettre g Les procédures de recours du droit public et les procédures de recours administratif

Les procédures de recours administratif sont des procédures juridictionnelles devant l'*administration fédérale* et devant le *Conseil fédéral*. Elles sont exhaustivement réglées par la loi sur la procédure administrative (RS 172.021); c'est pourquoi la loi sur la protection des données ne régit pas non plus ce domaine. L'exception ne vaut cependant que pour les *procédures administratives de deuxième instance*. La non application de la loi sur la protection des données aux procédures administratives de première instance, au sens de la loi sur la procédure administrative, n'aurait pas été sans faire courir de grands risques aux personnes concernées: la plupart des activités administratives auraient été privées de protection des données. La loi sur la procédure administrative régit en effet toutes les causes administratives qui débouchent sur une décision. Du moment que la plupart des activités administratives sont susceptibles d'aboutir à une décision, il eût été très facile aux organes fédéraux d'échapper aux obligations qui leur incombent en vertu de la protection des données. De même qu'aux recours administratifs, et pour les mêmes raisons, la loi sur la protection des données ne s'applique pas aux recours de droit public devant le Conseil fédéral (ces cas sont très peu nombreux, cf. art. 73 de la loi sur la procédure administrative).

Lettre h Les registres publics

L'exclusion des registres publics relatifs aux rapports juridiques de droit privé répond à des considérations semblables à celles qui ont présidé à l'exclusion des procédures juridictionnelles pendantes. L'exception instituée par la lettre h vise le

registre foncier, les registres de l'état civil, les registres des régimes matrimoniaux, le registre du commerce, le registre des bateaux, le registre des aéronefs, les registres concernant la poursuite pour dettes et faillite, le registre des réserves de propriété ainsi que les registres des brevets d'invention et des dessins, le registre de la protection des obtentions végétales, le registre des modèles industriels et le registre des marques de fabrique et de commerce. Ces registres sont principalement des banques de données tenues et garanties par l'Etat; ils renferment des informations indispensables sur la constitution, l'état, la modification et l'exercice de droits privés. Les traitements de données y relatifs sont régis par des prescriptions très précises et formalistes. Sécurité juridique oblige, il n'est pas question de les modifier par la loi sur la protection des données.

Outre les cas énoncés dans les lettres c à h, plusieurs autres textes législatifs prévoient des dispositions spécifiques régissant le traitement des informations et la protection des données. Lorsque de telles dispositions entrent en conflit avec la loi sur la protection des données, il appartient à l'interprète de résoudre ce conflit. De manière générale la loi sur la protection des données aura la préférence. En effet cette loi, de par son caractère général, couvre l'ensemble des activités des secteurs privé et public. Toutefois, il peut aussi arriver que des dispositions spéciales contiennent des normes de protection des données plus sévères ou mettent en place un système autonome de protection des données; dans de tels cas, ces normes l'emporteront exceptionnellement sur la loi.

Article 3 Définition

Lettre a Données personnelles

Par données personnelles (données), on entend toutes les informations qui se rapportent à une personne, physique ou morale, identifiée ou identifiable. Ces informations peuvent prendre la forme de mots, d'images ou de signes. Une personne est *identifiée* lorsqu'il ressort directement des informations détenues (p. ex. une pièce d'identité) qu'il s'agit d'une personne déterminée et d'elle seule. Une personne est *identifiable* lorsque, par corrélation indirecte d'informations tirées des circonstances ou du contexte, on peut l'identifier (p. ex. lorsque, à partir de données concernant des biens immobiliers, on peut remonter au propriétaire). Une possibilité purement théorique n'est cependant pas suffisante pour admettre la possible identification. En effet, si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre (p. ex. parce qu'il lui faudrait procéder à une analyse sophistiquée d'une statistique), on ne peut guère parler de possibilité d'identification³⁰⁾.

Lettre b Personne concernée

On entend par personne concernée, la personne au sujet de laquelle des données sont traitées. La personne concernée est le bénéficiaire direct de la loi. Toute personne physique ou morale, qu'elle ressortisse au droit privé ou au droit public, peut prétendre à la qualité de personne concernée (cf. nos commentaires concernant l'art. 1^{er}).

Lettre c Personnes privées

L'expression «personnes privées» au sens de la présente loi désigne avant tout les

personnes physiques ou morales de droit privé qui traitent des données. Sont aussi considérées comme personnes privées les personnes de droit public qui agissent selon le droit privé.

En présence d'*organes* mis en place par le droit privé, on se demandera si leur statut juridique relève du droit privé ou du droit public. Si l'organe en question est, pour l'essentiel, considéré comme ressortissant au droit public, on lui appliquera, en lieu et place de la partie privée de la présente loi, le cas échéant, le droit cantonal de protection des données. Il en va ainsi, par exemple, du tuteur. Ses tâches étant réglées par le code civil, on pourrait, en accord avec la jurisprudence du Tribunal fédéral³¹⁾, considérer qu'il s'agit d'une personne privée. Cependant, étant donné que la relation entre le tuteur et le pupille est, pour l'essentiel, un acte d'autorité, que le tuteur est soumis à une surveillance étatique et que ses actes sont susceptibles de recours, il doit être considéré comme un organe public du point de vue de la loi sur la protection des données³²⁾. Il s'ensuit qu'il doit être soumis au droit de la protection des données du canton qui fixe son statut juridique. Se basant sur ses compétences de droit privé, la Confédération pourrait certes régler la protection des données dans ce secteur de manière uniforme. L'opportunité d'une telle solution devra être examinée dans le cadre de la révision du droit de tutelle.

Lettre d Organes fédéraux

Sont considérés comme des organes fédéraux, les départements et les offices fédéraux, ainsi que leurs divisions et sections. Par organes fédéraux, on entend également les établissements et régies fédérales – notamment les CFF et les PTT – de même que les commandements militaires. Cette définition vise également toutes les personnes physiques et morales qui exécutent des tâches publiques pour le compte de la Confédération, telles les entreprises d'économie mixte et les corporations de droit public. Conformément au droit public suisse, les cantons et les communes ne sont pas considérés comme des organes fédéraux, et ce, même s'ils exécutent des tâches fédérales.

Lettre e Données sensibles

Les menaces qu'un traitement de données fait courir à la personnalité ou aux droits fondamentaux d'une personne ne dépendent pas seulement du but et de l'ampleur du traitement considéré, mais également du genre de données traitées. Certaines données ont, en tant que telles, une importante répercussion sur la personnalité des personnes concernées; notamment celles qui relèvent du domaine personnel secret ou de la vie privée, ou encore celles qui affectent la réputation ou le crédit d'une personne. Le projet soumet ce genre de données, du moins en partie, à un régime juridique spécial (cf. art. 7, 2^e al., 9, 2^e al., 14, 2^e al., 16, 1^{er} al., 29).

Le chiffre 1 vise non seulement les opinions ou les activités religieuses, philosophiques, politiques ou syndicales, mais également l'appartenance à une association qui prône des opinions de cette nature. *Le chiffre 2* range parmi les données sensibles les informations sur la «santé», la sphère intime ou l'appartenance à une race. Le terme santé est d'une acception plus étroite que l'expression *état psychique, mental ou physique*, utilisée dans le projet soumis à consultation en

1983. Celle-ci comprend notamment la taille et la couleur des yeux ou des cheveux, alors que le terme santé recouvre toute information médicale qui peut donner une image négative de la personne concernée. On entend par *sphère intime*, des données qui ont une grande connotation affective et que la personne concernée entend ne porter à la connaissance que de proches. Cette expression, qui ne doit pas être entendue dans le sens allemand de vie sexuelle, ne va cependant pas jusqu'à comprendre la situation financière d'une personne. Si les données concernant l'*appartenance à une race* ont été incluses dans le cercle des données sensibles, c'est en conformité, d'une part, avec la Convention du Conseil de l'Europe sur la protection des données et, d'autre part, avec les exigences en matière d'échanges internationaux de données. Par *mesure d'aide sociale au sens du chiffre 3*, on entend surtout les prestations des assurances sociales en rapport avec la maladie et l'accident, de même que la tutelle et l'assistance sociale. Enfin, les poursuites et les condamnations relevant du droit pénal commun ne sont pas les seules *poursuites et sanctions pénales ou administratives* visées par le *chiffre 4*; le sont également les procédures disciplinaires, les procédures de retrait de permis et l'exécution des peines.

En règle générale, les chiffres 1 à 3 ne concernent que les seules personnes physiques. Encore que des sociétés à but idéal exerçant accessoirement une activité économique ou des personnes morales condamnées pénalement³³⁾ puissent aussi entrer en considération.

L'énumération des données sensibles est exhaustive.

Lettre f Profils de la personnalité

La constitution, l'appréciation ou la communication à des tiers de profils de la personnalité requièrent une protection particulière. Par profil de la personnalité, on entend un assemblage de données relatives aux traits de la personnalité, aux compétences professionnelles ou aux activités extra-professionnelles, assemblage susceptible de donner une *image complète d'une personne ou de ses caractéristiques essentielles*. Des profils de la personnalité sont fréquemment, par exemple, élaborés lors de contrôles de sécurité ou de procédures d'engagement de personnel. La réunion d'informations sur les habitudes d'achat ou sur les qualifications scolaires ou professionnelles suffit à constituer un profil, certes partiel, de la personnalité des personnes concernées. La collecte de données en soi non sensibles – par exemple sur des références de lecture, sur des habitudes de voyage ou sur les loisirs en général – peut dévoiler des aspects secrets d'une personnalité, telle sa vision du monde. Les infinies possibilités d'analyse qu'offre l'informatique, à commencer par l'interconnexion de fichiers automatisés, ont considérablement facilité la constitution de profils de la personnalité. Souvent, les personnes concernées ignorent jusqu'à l'existence même de ces profils, et partant, ne sont pas en mesure de vérifier leur exactitude ou de s'enquérir de leur usage. Aussi, les profils de la personnalité privent-ils la personne concernée de la liberté de donner d'elle-même l'image qu'elle souhaite. De ce fait, ils portent une grave atteinte à l'épanouissement de la personnalité. On comprend dès lors qu'à l'instar des données sensibles, ils soient soumis à un régime juridique spécial: on ne pourra en effet constituer ou traiter des profils de la personnalité qu'à certaines conditions bien précises.

La notion de traitement est entendue dans un sens très large: elle comprend *toute opération relative à des données*, en particulier *chacune des diverses phases du traitement*. Elle englobe également la simple conservation des données, voire leur archivage, car même à ces stades du traitement des atteintes à la personnalité sont possibles, par exemple si la sécurité des données laisse à désirer. Toutefois, la mise aux Archives fédérales des documents pourra faire l'objet d'une réglementation spéciale (cf. art. 30, 2^e al.). La lettre h fait de la *communication* une forme particulière du traitement, et ce, pour deux raisons: premièrement, nous avons affaire, assurément, à la phase la plus dangereuse; deuxièmement, il est nécessaire d'exemplifier les diverses formes de communication possibles. Ainsi, on est en présence d'une communication, à chaque fois que des données ont été rendues accessibles d'une manière ou d'une autre. Tel est le cas de l'accès à un fichier au moyen d'une liaison en ligne, de la copie de bandes magnétiques ou, tout simplement, de la transmission de données extraites d'un fichier. Le projet prévoit en outre d'autres dispositions régissant la communication (cf. art. 7, 2^e al., let. b, 8, 16). La notion de traitement au sens du projet englobe toujours celle de communication. Par ailleurs elle recouvre non seulement les traitements automatisés mais aussi les traitements manuels, de même que toutes les formes mixtes.

Lettre i Fichiers

Les fichiers ont notamment deux fonctions: d'abord ils rassemblent les informations personnelles en cours de traitement, ensuite ils assurent leur conservation à long terme. A l'existence d'un fichier sont liées deux institutions spécifiques du droit de la protection des données: d'une part le droit d'accès, d'autre part l'obligation de déclarer un fichier (art. 5 et 7).

Est un fichier au sens de la présente loi, tout ensemble de données qui se rapporte à plus d'une personne. L'organisation et la structure du fichier ne jouent aucun rôle; ce qui est décisif, du point de vue de la protection des données, c'est que l'on puisse rechercher les données par personne concernée. S'agissant des traitements automatisés, il n'est pas nécessaire que les clés d'accès soient constituées par des noms de personnes, tant les possibilités d'interrogation de ces banques de données sont nombreuses. La catégorie des fichiers manuels ne comprend pas seulement les cartothèques ou les registres qui sont ordonnés par personne, mais aussi les registres dont l'accès par personne n'est possible qu'au moyen d'un index. En revanche, ne sont pas considérés comme des registres les ensembles de données qui, bien que permettant d'accéder à des données personnelles, nécessitent la mise en œuvre de moyens disproportionnés. Il en est ainsi notamment des millions de déclarations douanières qui sont conservées pendant un certain temps dans les différentes douanes de Suisse mais qui ne sont pas classées nominalement.

Lettre k Maître du fichier

L'expression désigne aussi bien une personne physique ou morale que l'organe fédéral qui, au regard du droit de la protection des données, est responsable du traitement des données personnelles contenues dans un fichier, et qui, de ce fait, est tenu de donner des renseignements et de déclarer le fichier. Est un maître de

fichier, celui qui décide du but du fichier et détermine les moyens et les méthodes de traitement (le matériel et le logiciel), peu importe qu'il soit ou non en mesure de disposer des données contenues dans le fichier.

S'agissant du *secteur privé*, la loi régit tant les personnes physiques que les personnes morales comme maîtres de fichier. Cette expression recouvre également les grandes entreprises très compartimentées. Dans ces derniers cas, il ne sera pas toujours aisé de déterminer à qui il incombe de remplir les obligations liées à la qualité de maître de fichier. Les grandes entreprises devront toutefois veiller à ce que la personne concernée soit toujours en mesure d'obtenir toutes les données détenues sur son compte. Pour des raisons pratiques, elles auront très souvent intérêt à s'informer auprès du requérant de la portée exacte de sa demande: concerne-t-elle simplement une filiale? ou un secteur d'activité déterminé? Ce problème ne devrait pas se poser dans le secteur public, car les organes fédéraux sont tenus de faire enregistrer tous leurs fichiers. A l'occasion de la déclaration aux fins d'enregistrement, ils pourront en effet indiquer auprès de quelle personne le requérant peut adresser sa demande. Il en va de même pour les fichiers, relevant du droit privé, qui doivent être déclarés.

En cas de traitement effectué par un tiers, il importe de déterminer qui du mandant ou du mandataire est le maître du fichier. A cet effet, on se demandera lequel des deux est en fin de compte responsable du traitement; ce sera normalement celui qui fournit les données. Si la tâche du centre de calcul se limite à mettre à disposition l'infrastructure technique permettant de faire subir à un ensemble préconstitué de données un traitement précis, le mandant demeure le maître du fichier. Tel est le cas du médecin qui confie la gestion de ses honoraires à une caisse de recouvrement. En revanche, l'institut qui, sur mandat, procède à des études de marché, doit être considéré comme le responsable des données récoltées. Il en va de même du détective privé qui a reçu pour tâche de recueillir des informations sur une certaine personne, car son mandant ne dispose pas lui-même des données.

Lettre l Participant à un fichier

On entend par participant au fichier, la personne ou l'organe fédéral qui, alors même qu'il n'est pas en droit de déterminer le but ou la structure du fichier, est néanmoins habilité à traiter certaines données du fichier. Un exemple: le registre central des étrangers. Bien que la responsabilité de ce fichier incombe à l'Office fédéral des étrangers, les divers services de contrôle des habitants et de police des étrangers disposent chacun d'une liaison en ligne leur permettant de modifier les données à volonté. On ne confondra pas la catégorie des participants à un fichier et celle des *destinataires des données*; ces derniers, s'ils sont habilités à avoir connaissance des données, ne sont en revanche pas en droit de les modifier ou de les détruire.

221.2 Section 2: Les dispositions générales de protection des données

Article 4 Principes

L'article 4 définit succinctement les principes fondamentaux de la protection des

+ données; il s'agit là du *noyau dur* de la loi. Ces principes régissent ceux qui traitent les données tant à titre privé qu'à titre public. Toute personne qui *traite des données à titre privé* commet une atteinte à la personnalité s'il transgresse l'un ou l'autre de ces principes fondamentaux sans juste motif (cf. art. 9, 2^e al., let. a). En d'autres termes, ces principes fondamentaux précisent à quelles conditions un traitement effectué par une personne privée porte atteinte à la personnalité. S'agissant des *organes publics*, la portée de ces principes fondamentaux est encore plus grande: ils constituent des normes de comportement directement applicables; la personne concernée peut recourir contre leur violation.

1^{er} alinéa Modalités de la collecte des données

Ceux qui traitent des données, à titre privé ou à titre public, sont en droit de collecter des données à chaque fois qu'un traité de droit international public, une loi, un arrêté fédéral de portée générale ou une ordonnance le prévoit. Reste qu'en général la collecte de données effectuée par des privés n'est pas délimitée spécialement. Dès lors, à côté des dispositions générales s'opposant à la collecte qui peuvent le cas échéant trouver application, un principe revêt ici une importance particulière: les données doivent être traitées conformément à la bonne foi. Les données ne doivent pas être collectées à l'insu de la personne concernée ou contre sa volonté. Celui qui recueille des données en trompant intentionnellement la personne concernée – par exemple en se présentant sous une fausse identité ou en donnant de fausses indications quant au but du traitement – transgresse le principe de la bonne foi (cf. art. 28 CO). Il en va de même de celui qui collecte des données *clandestinement*, par exemple en écoutant les conversations ou en épiant des personnes³⁴⁾, ou encore en manipulant les programmes d'un système de communication interactif (vidéotex). Remarquons au passage qu'une telle collecte peut en outre constituer une infraction pénale. Enfin, il ne fait aucune doute qu'il est illicite de collecter des données par la menace, par astuce ou en usant de violence: ces procédés tombent en effet sous le coup du droit pénal.

Selon la quatrième section de la présente loi, les *organes fédéraux* doivent se plier à une condition supplémentaire: la collecte des données doit en principe être effectuée de façon reconnaissable pour les personnes concernées (art. 15).

2^e alinéa Exactitude des données

Le traitement de données inexactes peut porter gravement atteinte aux personnes concernées. Et des erreurs minimales peuvent déjà causer de grands dommages. Ainsi, une caisse de recouvrement, qui aurait confondu deux personnes portant le même nom et habitant dans la même rue, peut être amenée à engager à tort des poursuites contre une personne qui n'est pas son débiteur. L'exactitude au sens de la présente loi n'implique pas seulement que les données doivent contenir des affirmations exactes, mais aussi qu'elles doivent être complètes et à jour, du moins autant que les circonstances le permettent. Il est inutile de préciser que le chef du personnel qui déplace ou congédie un employé sur la base d'un certificat médical périmé peut porter atteinte à la personnalité de ce dernier. De même, l'évaluation du crédit d'une personne divorcée peut être faussée si les pièces produites à cet effet omettent de mentionner le remariage de son ex-conjoint, et partant l'extinction de l'obligation d'entretien. Ces exemples démontrent à l'envi que l'on ne

peut se prononcer dans l'abstrait sur l'exactitude d'une donnée; il faut à chaque fois prendre en considération les circonstances du cas d'espèce.

3^e alinéa Proportionnalité du traitement

Les organes publics sont tenus de respecter le principe de proportionnalité; du fait de cet alinéa, ce principe devient également applicable au secteur privé. En conséquence, quiconque traite des données est obligé de ne collecter et de ne traiter que les seules données qui lui sont nécessaires et aptes à atteindre un but déterminé. Ainsi, une agence de location d'automobiles est en droit de relever l'identité et l'adresse du preneur; il serait toutefois excessif de contraindre celui-ci à fournir des renseignements sur ses relations familiales ou sur ses rapports avec des tiers. Ces informations peuvent en revanche être indispensables à l'évaluation du crédit d'une personne. Reste que même dans ce cas, il serait exagéré de se renseigner sur ses convictions religieuses ou ses appartenances politiques.

En outre, il faut toujours procéder à une pondération des intérêts entre le but du traitement et l'atteinte nécessaire à la personnalité. C'est ainsi que dans le cadre d'une campagne électorale, il ne se justifie pas de dévoiler complètement et systématiquement la vie privée d'un adversaire politique.

4^e alinéa Modifications du but initial

Etant donné que les systèmes d'informations modernes ont décuplé les possibilités d'utiliser et de communiquer des données, le danger est toujours plus grand que des données soient utilisées à des fins autres que le but initial. Le principe de la bonne foi en affaires commande que toute personne concernée par un traitement de données sache à quelles fins les informations sur son compte sont traitées. Le plus souvent, ces informations n'ont pas été données inconditionnellement, mais en vue d'un traitement déterminé, voire même uniquement dans ce but. Il s'ensuit que les données ne doivent en principe être utilisées que dans le but qui a été indiqué lors de la collecte ou qui ressort des circonstances. Cela signifie, par exemple, que les adresses obtenues à l'occasion d'une récolte de signatures à l'appui d'une initiative, ne peuvent pas être utilisées à des fins commerciales; autrement dit, les auteurs de l'initiative ne sont pas en droit d'en tirer parti pour envoyer de la publicité aux signataires. Il ne serait pas non plus tolérable que les services du personnel de l'administration fédérale communiquent à une maison de vente par correspondance les adresses des fonctionnaires dont le traitement atteint un montant déterminé. Enfin, il serait tout aussi inacceptable d'analyser systématiquement les données enregistrées dans le système videotex pour se faire une opinion des habitudes d'achat et des intérêts d'une personne.

Toutefois, il est possible de modifier le but initial si une *norme juridique le prévoit*. Ainsi, une disposition légale peut habiliter une autorité à accéder aux informations détenues par une autre autorité. Cette exception a une double justification; premièrement, elle a été voulue par le législateur, autrement dit par un organe élu démocratiquement; deuxièmement, du fait du principe de la publicité des lois, la personne concernée est censée savoir à quoi s'attendre.

5^e alinéa Communication de données à l'étranger

Des données, dont le traitement en Suisse ne pose aucun problème, peuvent

cependant mettre en danger la personne concernée, si elles sont communiquées à l'étranger. Que l'on songe à des informations transmises à des Etats, dont le gouvernement ne respecterait pas les droits de l'homme, sur leurs ressortissants établis en Suisse ou encore à une entreprise suisse qui communique à sa filiale à l'étranger des informations sur un employé appartenant à une communauté religieuse persécutée dans ce pays³⁵). Celui qui entend communiquer des données à l'étranger, voire même dans certains cas, à des *organisations internationales* doit être conscient de ces dangers et en tirer les conséquences. Dans de nombreux cas, toutefois, il n'est guère aisé d'évaluer exactement l'étendue du danger. C'est pourquoi le projet ne considère comme illicite que les communications de données qui pourraient causer une *grave* atteinte à la personnalité. Cette restriction a pour conséquence que les échanges internationaux de données ne seront pas entravés outre mesure; en particulier, les communications qui ont un caractère essentiellement personnel ou familial ne seront pas touchées.

Il y a notamment une atteinte grave à la personnalité, si des données sont transmises dans un pays qui ne protège pas les données dans une mesure semblable au droit suisse. Pour apprécier le degré de similitude de la protection, on examinera si l'Etat en question respecte les principes fondamentaux posés par l'article 4, si la personne concernée a le droit d'accéder à ses données et si, le cas échéant, elle peut en obtenir la rectification ou la destruction. Des conditions que remplissent très certainement la plupart des Etats qui connaissent une législation sur la protection des données, à tout le moins ceux qui ont ratifié la Convention n° 108 du Conseil de l'Europe. Reste que la grande majorité des Etats du globe ne dispose pas encore d'une loi sur la protection des données; partant, le critère de l'existence d'une législation pertinente n'est pas suffisant. Dans nombre de cas, il sera nécessaire de procéder à une évaluation d'ensemble de l'ordre juridique, de la pratique des tribunaux et de l'organisation de l'administration de l'Etat considéré. Au demeurant, celui qui traite les données a toujours la possibilité de pallier l'absence de garanties institutionnelles en matière de protection des données par le biais de dispositions contractuelles destinées à assurer la protection voulue.

6^e alinéa Sécurité des données

Certains problèmes de protection des données peuvent être évités, si l'on prend, à temps, les mesures de sécurité qui s'imposent. Les systèmes informatiques modernes, tout particulièrement, requièrent des mesures d'*aménagement des lieux*, empêchant à tout tiers non autorisé d'accéder aux équipements informatiques. Des mesures *techniques* peuvent également être nécessaires pour prévenir les pannes (p. ex. à la suite d'une coupure de courant) et, partant, la destruction irrémédiable des données. Enfin, on veillera à ce que les données ne soient pas accessibles à n'importe qui et à ce que les principes fondamentaux de la protection des données soient respectés par des mesures *organisationnelles*, telles des procédures d'identification des usagers, des évaluations périodiques, des mesures de sécurité ou encore la nomination d'un responsable de la protection des données au sein de l'entreprise.

Etant donné la grande diversité des techniques de traitement des données, le projet renonce à réglementer dans le détail les mesures de sécurité envisageables.

Il appartiendra à ceux qui traitent les données, le cas échéant aux organisations professionnelles qui les représentent, de déterminer les mesures de sécurité propres à leur domaine d'activité et de prendre les dispositions adéquates. A défaut, le Conseil fédéral se fondera sur son pouvoir réglementaire (art. 30, 1^{er} al.), pour poser des exigences minimales. Quant aux divers secteurs d'activité de l'administration fédérale, ils seront régis par des prescriptions de sécurité spécifiques.

Article 5 Droit d'accès

Le droit d'accès est l'institution-clef de la protection des données. Sans droit d'accès, la personne concernée ne serait pas en mesure de faire valoir effectivement ses prétentions en matière de protection des données. Seul celui qui a connaissance des données qui sont traitées sur son compte est à même, le cas échéant, de les faire rectifier ou de les faire détruire, ou, à tout le moins, d'en contester l'exactitude (cf. art. 12 et 22).

Suivant le 1^{er} alinéa, tout un chacun est habilité à requérir l'accès à un fichier. Le droit d'accès est un droit subjectif strictement personnel. Il s'ensuit qu'un mineur ou un interdit capables de discernement peuvent exercer ce droit sans le consentement de leur représentant légal (cf. art. 19, 2^e al., CC). Autre conséquence du caractère strictement personnel du droit d'accès, nul ne peut y renoncer par avance (6^e al.). Le droit d'accès ne peut pas s'exercer à l'encontre de n'importe quelle personne qui traite des données, mais seulement à l'encontre du *maître d'un fichier*. Un ensemble de données classifié de manière systématique fait en effet courir beaucoup plus de risques à la personnalité des personnes concernées qu'un agrégat de données que l'on ne peut rechercher par personne concernée. De surcroît, instituer un droit d'accès à l'encontre de tout traitement de données, et non seulement à l'encontre des données contenues dans un fichier, aurait été irréaliste, car ceux qui traitent les données auraient souvent été contraints de procéder à des recherches considérables. Enfin, il va de soi qu'on ne peut accéder qu'à ses *propres* données; un droit d'accès plus étendu ouvrirait la porte à de nouvelles atteintes à la personnalité.

Le 2^e alinéa définit les composantes du droit d'accès. Préalable indispensable, le maître du fichier devra d'abord examiner si le fichier contient des données sur le compte du requérant. Dans la négative, il en informe le requérant et l'affaire s'arrête là. Dans l'affirmative, en revanche, il lui communique les données pertinentes (let. a). Les renseignements fournis devront être *exacts et complets*. L'octroi de renseignements partiels n'est admissible que si la loi le prévoit (cf. art. 6) ou si la personne concernée a expressément déclaré s'en contenter. En outre, le requérant doit être informé du *but du traitement*; sans quoi, il ne peut être à même d'évaluer les risques que lui fait courir le traitement. De surcroît, on donnera au requérant connaissance de la *base légale* du traitement. Cette dernière obligation incombera surtout aux organes fédéraux; elle pourra cependant également concerner les personnes privées qui exécutent des obligations légales, par exemple les employeurs obligés d'effectuer des décomptes AVS. En outre, le maître du fichier est tenu de communiquer les *catégories de données traitées*, de *participants au fichier* et de *destinataires des données* (let. b). En revanche, il n'est pas obligé de désigner *nommément* les *participants* et les *destinataires*. Il importe de ne pas

imposer au maître du fichier un volume de travail excessif ou de le contraindre à dévoiler ses relations d'affaires. La nouvelle loi n'oblige pas non plus le maître de fichier à révéler la *source* de ses données. L'expérience le démontre à l'envi: soit on ne peut s'acquitter de cette obligation qu'au prix d'un important volume de travail, soit la connaissance des sources d'une donnée n'apporte pas grand chose. Du reste, il est justifié de ne pas contraindre les médias à révéler l'identité d'un informateur avant la publication de l'information. Cela ne signifie cependant pas que la personne concernée soit privée de tout moyen de connaître la source des données. Suivant la jurisprudence du Tribunal fédéral relative à l'article 4 de la constitution, la personne concernée peut accéder à son dossier non seulement au cours d'une procédure pendante, mais également en dehors de toute procédure formelle, pour autant qu'aucun intérêt public ou privé au maintien du secret ne s'y oppose³⁶; cette jurisprudence ne peut toutefois être invoquée qu'à l'égard des autorités étatiques.

Le 3^e alinéa traite de ce que le corps médical appelle les *éclaircissements dommageables*. Il y a éclaircissement dommageable, lorsqu'on révèle à un patient, qui n'y est pas préparé, la vérité sur son état de santé, lequel se détériore à la suite de ces révélations. Nous sommes d'avis qu'il n'appartient pas au maître du fichier de décider si un renseignement peut ou non porter préjudice aux personnes concernées. Le requérant doit évaluer lui-même les risques que l'octroi du renseignement lui fait courir. Reste qu'une exception s'impose: elle concerne les informations sur l'état de santé. Il n'est cependant pas question de permettre au maître du fichier – ce peut être une caisse-maladie – d'invoquer le risque d'un éclaircissement dommageable pour refuser l'accès. Le maître du fichier sera toutefois en droit de confier à un médecin le soin de communiquer à la personne concernée des renseignements sur sa santé. Seul un médecin en effet est à même d'informer la personne concernée avec tout le ménagement nécessaire. En conséquence, le 3^e alinéa n'est rien d'autre qu'une disposition destinée à protéger la personnalité de la personne concernée. Dans la mesure où le maître du fichier relève du droit public fédéral, cette règle doit être comprise comme une exception aux dispositions sur la communication prévues par l'article 16.

Le 4^e alinéa vise à empêcher que les règles sur le droit d'accès soient tournées: le maître du fichier ne saurait échapper à ses obligations en confiant à un tiers le soin de traiter ses données. Il lui est cependant loisible de charger son mandataire, par exemple un centre de calcul, d'octroyer à sa place le renseignement. Cela dit, le mandataire lui-même est tenu d'octroyer le renseignement dans deux cas: lorsqu'il refuse de révéler l'identité du maître du fichier ou lorsque ce dernier a son domicile à l'étranger. Ainsi, il y aura toujours quelqu'un pour octroyer le renseignement. Le titulaire du droit d'accès est dispensé ainsi de procéder à de longues recherches sur l'identité du maître du fichier, ce qui lui évite également de devoir ouvrir action à l'étranger.

Le 5^e alinéa dispose que le renseignement doit être octroyé par écrit et gratuitement. Le Conseil fédéral peut toujours prévoir des exceptions à ces deux principes. Dans certains cas, il peut se révéler judicieux de permettre au requérant de consulter ses données directement à l'écran et parfois même de lui ouvrir le dossier complet. Il importe cependant de veiller à ce que le maître du fichier ne soit pas sollicité sans cesse: à cet effet, il est probable que l'ordonnance

d'exécution contraindra celui qui entend exercer son droit d'accès plus d'une fois dans un laps de temps déterminé, par exemple une année, à s'acquitter d'un émolument. Il pourra en aller de même si l'octroi des renseignements occasionne un volume de travail excessif, par exemple parce que les pièces ont déjà été versées aux archives.

Article 6 Restrictions du droit d'accès

Si inaliénable et essentiel pour la protection de la personnalité qu'il soit, le droit d'accès ne saurait être exercé sans limites. Vu qu'il s'agit là d'un droit strictement personnel, l'article 6 ne peut énumérer les motifs de restriction de ce droit que de manière exhaustive. De surcroît, cette disposition doit être interprétée limitativement; en d'autres termes, le droit d'accès ne doit être restreint que si cela est vraiment indispensable. Par restrictions du droit d'accès, on entend non seulement le refus de principe d'octroyer un renseignement, mais également un octroi partiel, voire un octroi différé dans le temps. Si ce choix s'offre à lui, le maître du fichier devra opter pour la solution la plus favorable à la personne concernée. Pour le reste, l'article 6 est en grande partie calqué sur la réglementation du refus de témoigner instituée par la loi sur la procédure administrative (art. 27, RS 172.021).

Les différents motifs de restriction définis par le *1^{er} alinéa*, appellent les remarques suivantes:

L'existence d'une loi au sens formel – ce qui englobe aussi les traités internationaux et les arrêtés de portée générale – comme motif de restriction concerne avant tout les maîtres de fichiers soumis au droit public (let. a). A ce propos, on relèvera que l'article 13 de la loi sur l'organisation de l'administration (RS 172.010) dispose que les débats du Conseil fédéral ne sont pas publics. Se fondant sur cette disposition, le Conseil fédéral peut refuser l'accès aux procès-verbaux de ses séances. Signalons enfin que le motif de restriction institué par la lettre a sera rarement applicable aux maîtres de fichiers relevant du secteur privé.

Par *intérêt public prépondérant*, au sens de la lettre b, on entend avant tout la sûreté intérieure ou extérieure de la Confédération. Par sûreté extérieure, il faut comprendre non seulement le respect des obligations de droit international public, mais aussi le maintien de bonnes relations avec l'étranger. Cette disposition permettra, par exemple, de refuser l'accès aux fichiers du Ministère public si l'octroi du renseignement risque de dévoiler des méthodes ou des résultats d'investigation. De même, l'accès aux fichiers du Département fédéral des affaires étrangères pourra être refusé si des négociations en cours avec des Etats étrangers en étaient compromises; ce serait également le cas si les informations recherchées concernaient une personne dont la Suisse assure la protection en vertu du droit international.

L'accès peut également être refusé si l'octroi des renseignements risque de compromettre *une instruction pénale ou une autre procédure d'instruction* telle qu'une procédure disciplinaire (let. c). Cette disposition ne devrait en pratique guère jouer de rôle puisque la loi ne s'applique pas aux procédures qui sont réglementées par une loi de procédure (cf. art. 2). Il n'est cependant pas exclu que certains renseignements obtenus hors du cadre de l'instruction puissent avoir des

conséquences négatives sur celle-ci; l'inculpé qui souhaite accéder au fichier de ses dénonciateurs en est un exemple.

L'intérêt supérieur du maître du fichier peut également justifier une restriction du droit d'accès (let. d). Cette disposition concerne avant tout le secteur privé. Ainsi, un grand magasin peut refuser l'accès au registre des clients suspectés de vol. Un maître de fichier qui craint que le requérant ne s'adonne à l'espionnage économique peut également s'opposer à l'accès.

Il est également possible de restreindre le droit d'accès lorsqu'il y a fort à craindre que le requérant ne tire parti de son droit pour rassembler des informations sur une tierce personne et, partant, *ne risque de porter atteinte aux intérêts de cette tierce personne* (let. e). Un exemple: le preneur d'un contrat d'assurance n'a pas nécessairement intérêt à ce que le tiers bénéficiaire en ait connaissance.

Suivant le 2^e alinéa, toute restriction du droit d'accès doit être motivée. Conformément aux principes généraux de la procédure administrative, les organes fédéraux sont tenus de signifier une restriction au droit d'accès par voie de décision. Aucune prescription de forme n'est en revanche imposée aux *personnes qui traitent des données* à titre privé; il serait cependant opportun qu'ils motivent leurs restrictions par écrit. La teneur de la motivation doit permettre au requérant d'apprécier la légitimité de la restriction. Reste que dans certains cas, notamment lorsque la sûreté intérieure ou extérieure de la Confédération est en jeu, on ne doit pas se montrer trop sévère quant à la teneur de la motivation; à défaut, le maître du fichier se verrait contraint de révéler indirectement ce qui devait être maintenu secret.

Article 7 Registre des fichiers

Le registre des fichiers est la pierre angulaire du droit d'accès. Suivant le 1^{er} alinéa, le registre, qui peut être consulté par tout un chacun, est tenu par le préposé fédéral à la protection des données.

Aux termes du 2^e alinéa, l'étendue de l'obligation de déclarer un fichier diffère selon que le maître du fichier relève du droit public ou du droit privé. Ainsi, tous les fichiers tenus par les organes fédéraux doivent être déclarés, exception faite des fichiers qui concernent la sûreté de l'Etat et la sécurité militaire (art. 21). Les maîtres de fichiers relevant du droit privé ne sont en principe pas tenus de déclarer ceux-ci. Font exception les fichiers qui contiennent des données sensibles ou des profils de la personnalité (let. a), ou ceux dont les données sont communiquées à des tiers; encore faut-il qu'aucune disposition légale n'oblige le maître du fichier à tenir le fichier considéré et que celui-ci soit tenu à l'insu des personnes concernées. Ainsi, un employeur ne sera pas obligé de déclarer le registre des salaires de ses employés, car ce registre est tenu en conformité à la législation sur l'AVS dans le but de communiquer les informations nécessaires aux organes compétents. Il ne sera guère aisé de déterminer dans chaque cas d'espèce la manière dont la personne concernée est censée avoir connaissance de l'existence d'un registre accessible à des tiers ou renfermant des données sensibles sur son compte. Il ne sera pas toujours nécessaire que le maître du fichier avertisse directement chaque personne enregistrée dans le fichier. Ainsi, une entreprise pourra se contenter d'annoncer l'existence d'un registre des employés par voie

d'affichage ou de circulaire, voire en donnant les informations adéquates à tout nouvel employé lors de l'engagement. Ce qui est décisif, c'est que la personne concernée soit au clair sur l'existence d'un fichier. Enfin, doit aussi être annoncé le traitement ou la communication qui présente un caractère périodique, c'est-à-dire qui se répète à intervalles réguliers. La réglementation contenue à l'article 7, 2^e alinéa, place le maître du fichier devant l'alternative suivante: soit il déclare le fichier, soit il informe les personnes concernées de l'existence de celui-ci. Reste que les grands fichiers, tels ceux que tiennent les entreprises de marketing direct ou les agences de renseignements, ne laissent pratiquement aucun choix: seul le premier terme de l'alternative entre en considération.

Suivant le 3^e alinéa, les fichiers doivent être déclarés avant d'être opérationnels. Le préposé sera ainsi en mesure de signaler d'emblée d'éventuels problèmes.

Aux termes du 4^e alinéa, il appartiendra au Conseil fédéral de régler, par voie d'ordonnance, les modalités de déclaration des fichiers. Il devra notamment déterminer quelles indications devront être fournies lors de l'enregistrement. Ces informations correspondent, pour l'essentiel, à celles qui doivent être communiquées à celui qui fait valoir son droit d'accès conformément à l'article 5, 2^e alinéa, lettre b. Le Conseil fédéral devra, en outre, décider sous quelle forme le registre sera publié et de quelle manière il pourra être consulté. De surcroît, l'ordonnance prévoira sa mise à jour périodique. Enfin, le Conseil fédéral pourra instituer des procédures de déclaration simplifiées, voire des exceptions à l'obligation de déclarer ou d'enregistrer, lorsque, selon toute probabilité, le traitement considéré ne menace pas la personnalité des personnes concernées.

On relèvera encore que la personne privée qui ne s'acquitte pas de son obligation de déclarer un fichier est passible de la peine prévue à l'article 28 du projet.

Article 8 Communication à l'étranger

Nous l'avons déjà dit (cf. nos remarques concernant l'art. 4, 5^e al.), la communication de données à l'étranger n'est pas dénuée de risques d'atteinte à la personnalité. Aussi le 1^{er} alinéa institue-t-il une obligation de déclarer certains transferts de données à l'étranger au préposé à la protection des données; celui-ci est ainsi en mesure, se fondant sur l'article 24, d'ouvrir une enquête, à tout le moins dans les cas les plus graves. Par étranger, on entend non seulement les Etats étrangers, mais également les organisations internationales. Ce qui est décisif en l'occurrence c'est que les données transférées se retrouvent soumises à un ordre juridique étranger. On assimilera la transmission de données au sein d'une entreprise multinationale à la communication de données à l'étranger. L'obligation de déclarer les communications de données à l'étranger est toutefois très limitée. Elle n'intervient que si les données sont communiquées *régulièrement ou en grand nombre*. L'obligation de déclarer les communications est écartée à chaque fois que la communication est prévue par la loi (let. a) ou que les personnes concernées en ont connaissance (let. b). Pour déterminer s'il y a connaissance ou non, on appliquera les mêmes critères qu'en matière d'exception à l'obligation d'enregistrer (cf. art. 7).

Suivant le 2^e alinéa, il appartiendra au Conseil fédéral de régler les modalités de la déclaration. Il lui incombera notamment de préciser le critère du «grand nombre

de données», tout en ayant à l'esprit que ce critère est d'ordre à la fois quantitatif et qualitatif. L'ordonnance d'exécution distinguera les données sensibles des autres: le plafond limite sera moins élevé dans le premier cas que dans le second. En outre, le Conseil fédéral pourra instituer des procédures de déclaration simplifiées pour les communications de données qui, bien qu'elles soient effectuées à l'insu de la personne concernée, ne portent pas atteinte à la personnalité. La communication de données non sensibles aux fins de recherche ou de statistique pourra notamment bénéficier de cette exception. Dans le même ordre d'idées, on pourra se contenter d'une déclaration globale lorsqu'on a affaire à une entreprise dont les activités s'étendent à plusieurs pays (p. ex., une compagnie aérienne).

On relèvera enfin que la personne privée qui ne s'acquitte pas de son obligation de déclarer tombe sous le coup des dispositions pénales instituées par l'article 28.

221.3 Section 3: Traitement de données personnelles par des personnes privées

Article 9 Atteintes à la personnalité

La partie consacrée au droit privé de la loi sur la protection des données complète et concrétise à la fois les dispositions du code civil sur la protection de la personnalité. L'article 28, 1^{er} alinéa, du code civil pose un principe général: celui qui est atteint illicitement dans sa personnalité peut faire appel au juge. La section 3 du projet concrétise ce principe dans le domaine particulier des traitements de données. Première disposition de cette section, l'article 9 spécifie certains cas d'espèces, autrement dit certains types de traitements, qui sont censés violer illicitement la personnalité si celui qui traite les données n'est pas en mesure de faire valoir un motif justificatif.

Le 1^{er} alinéa met l'ensemble des dispositions de la section 3 en corrélation avec l'article 28, 1^{er} alinéa, du code civil. Il est ainsi clairement exprimé que la loi sur la protection des données s'inscrit dans la droite ligne des principes établis par le code civil en matière de protection de la personnalité, pour autant qu'il s'agisse de traitements de données relevant du droit privé. En définitive, les deux législations visent le même but, à savoir sauvegarder et l'autonomie des personnes concernées et leur droit à se déterminer librement.

Le 2^e alinéa énonce divers traitements de données susceptibles de porter atteinte à la personnalité. Suivant la lettre a, quiconque viole les *principes généraux définis à l'article 4* porte atteinte à la personnalité. Ces principes constituent la colonne vertébrale de la législation sur la protection des données; partant, ils ne peuvent être transgressés sans raison majeure. Selon la lettre b, il y a également violation de la personnalité lorsque le traitement est effectué au *mépris de la volonté expresse de la personne concernée*. Il importe en effet de respecter le droit des personnes concernées à l'autodétermination individuelle en matière d'information, ce qui est une véritable nouveauté en droit privé. La personne concernée doit ainsi être en mesure de s'opposer inconditionnellement à un traitement, autrement dit sans avoir à justifier d'un intérêt particulier. Encore faut-il que l'opposi-

tion porte sur des cas d'espèce: la personne concernée n'est pas en droit de poser une interdiction générale. Dernière condition: l'interdiction doit être *expresse*. Cela ne signifie cependant nullement que celui qui traite des données en omettant de solliciter l'accord des personnes concernées porte atteinte à leur personnalité. A ce propos, il y a lieu de signaler l'existence de la liste dite «Robinson»; cette liste, établie par les marchands d'adresses, recense les personnes qui ont expressément manifesté la volonté de ne recevoir aucun envoi à caractère publicitaire. Inutile de préciser enfin que la personne concernée peut en tout temps retirer son opposition au traitement. Ce retrait peut, à la limite, prendre la forme d'une acceptation tacite du traitement. La lettre c définit un autre cas d'atteinte à la personnalité: *la communication à des tiers de données sensibles ou de profils de la personnalité*. Ces informations, qui soit sont très dommageables pour l'individu, soit en tracent un portrait détaillé, requièrent la plus grande confidentialité: elles ne doivent pas, par exemple, être communiquées sans motif justificatif, en particulier, sans le consentement de la personne concernée. A l'instar de la lettre b, cette disposition reprend l'idée de base de la loi: la personne concernée doit pouvoir déterminer quelles données la concernant doivent être traitées.

L'article 9 n'énumère *pas exhaustivement* les cas d'atteintes à la personnalité. En outre, la personne concernée peut invoquer à l'encontre de traitements de données illicites les droits que lui confèrent les dispositions destinées à protéger la personnalité contenues dans d'autres lois, (p. ex. la loi sur la concurrence déloyale³⁷).

Article 10 Motifs justificatifs

Aux fins de clarification, le 1^{er} alinéa reprend, dans les mêmes termes, le principe général posé par l'article 28, 2^e alinéa, du code civil: une atteinte à la personnalité n'est pas illicite, et partant n'entraîne aucune conséquence juridique, soit si la victime y a consenti, soit si celui qui traite les données peut faire valoir un intérêt prépondérant privé ou public, ou encore peut se fonder sur une disposition légale. Reste que la protection offerte par la loi à l'encontre des atteintes illicites causées par des traitements de données ne saurait être entière. Elle doit notamment s'effacer lorsque l'intérêt – privé ou public – au traitement est supérieur à l'intérêt à la protection de la personne concernée. Dans l'avant-projet, le texte de loi opérait lui-même la pesée des intérêts: certains traitements de données bénéficiaient de par la loi d'un motif justificatif, d'autres d'une présomption légale d'intérêts supérieurs. Nous vous proposons de renoncer à ce système, car sa rigidité ne permet pas de tenir suffisamment compte des cas d'espèce. De surcroît, sa complexité a fait l'objet de nombreuses critiques lors de la procédure de consultation. Enfin, il faut bien convenir que seul le juge est en mesure, à la lumière des faits, d'apprécier le caractère justifié ou non d'une atteinte à la personnalité.

Le 2^e alinéa pose les jalons qui permettront au juge de pondérer les intérêts en présence. Il n'appartient pas au législateur de se substituer au juge; cependant, il importe que le législateur lui fournisse des éléments d'appréciation pour les cas où le conflit entre l'intérêt au traitement des données et l'intérêt à la protection est particulièrement aigu. Les motifs justificatifs énoncés au 2^e alinéa sont en principe applicables non seulement aux cas d'atteintes à la personnalité définis à

l'article 9, mais encore aux atteintes à la personnalité qui ne sont pas spécifiées par le projet. Dans son appréciation, le juge sera, dans certains cas, plus volontiers enclin à admettre l'existence d'un motif justificatif; les atteintes à la personnalité du fait de données inexactes en sont assurément un exemple. En revanche, la collecte de données par des moyens illégaux sera rarement justifiable et celle par des moyens contraires à la bonne foi pratiquement jamais.

Le projet prévoit trois catégories de motifs justificatifs; la première regroupe certaines activités économiques: la conclusion d'un contrat, la concurrence économique et l'évaluation du crédit; la seconde, les besoins des médias à caractère périodique; la troisième, les traitements effectués dans un but ne se rapportant pas à des personnes.

La *lettre a* peut justifier une atteinte à la personnalité portée par une personne privée à son *cocontractant*, quelle que soit la nature du contrat. L'expression «en relation directe avec la conclusion d'un contrat» couvre aussi les traitements de données effectués au stade pré-contractuel. Ainsi, ce motif justificatif pourrait être invoqué par un vendeur désireux de se renseigner sur un client potentiel, ou encore par un bailleur qui souhaite s'informer sur un futur locataire. N'étant pas en relation directe avec la conclusion d'un contrat, les campagnes publicitaires ne bénéficient pas du motif justificatif institué par la lettre a, même si, en définitive, elles aboutissent à la conclusion du contrat. Le motif justificatif peut être invoqué à l'occasion de n'importe quelle forme de traitement: collecte ou évaluation des données, peu importe. Enfin, la portée du motif justificatif s'étend également à la communication à des tiers: celui qui traite des données sur son cocontractant pourra les transmettre à une filiale, à un livreur ou à un fournisseur.

La *lettre b* institue un motif justificatif se rapportant à la *concurrence économique*. Pour être compétitif, il faut détenir des informations économiques à jour, et partant, s'informer continuellement sur ses concurrents. Inversement, on doit s'attendre à ce que ses concurrents en fassent de même. Le *registre du commerce* assure déjà une certaine publicité qui s'accommode du jeu de la concurrence. Les personnes qui figurent dans ce registre lèvent, en partie du moins, le voile sur leurs activités commerciales; il est vrai qu'elles le font aussi dans le but de jouir d'un certain capital de confiance et de crédit. Dès lors, celui qui cause une atteinte à la personnalité en traitant des données concernant ce genre de personnes «publiques» devrait pouvoir bénéficier d'un motif justificatif. Entrent dans la catégorie de ces personnes «publiques» en premier lieu les sociétés de capitaux et les sociétés coopératives, de même que les raisons individuelles et les sociétés de personnes qui sont tenues de s'inscrire au registre du commerce³⁸). En revanche, cette catégorie ne comprend pas les personnes physiques qui sont inscrites au registre du commerce en qualité d'organes d'une personne morale. Le motif justificatif institué par la lettre b n'entre en considération que si les données sont traitées exclusivement à des fins *internes*, autrement dit ne sont pas communiquées à des tiers. Il appartiendra à la jurisprudence de préciser dans quelle mesure les échanges d'informations au sein d'un seul et même consortium doivent être considérés comme un traitement interne. A cet égard, il importera d'examiner si, en l'espèce, les informations demeurent au sein d'une seule et même unité économique. Enfin, le motif justificatif ne peut être invoqué que si les données et le genre du traitement sont en relation étroite avec la concurrence économique.

Pour les mêmes raisons, la lettre c institue un motif justificatif en faveur de ceux qui traitent des données *en vue d'évaluer le crédit* d'une entreprise commerciale. Dans une économie de marché, le crédit est un facteur essentiel. Lorsqu'on est inscrit au registre du commerce, on doit s'attendre à faire l'objet d'évaluations de crédit et, partant, tolérer, plus que d'autres, les atteintes à la personnalité. On ne peut toutefois invoquer le motif justificatif que si le traitement porte sur des données non sensibles. Cette restriction est nécessaire; en effet, contrairement à l'hypothèse prévue à la lettre b, les évaluations de crédit impliquent, très souvent, que les données soient communiquées à des tiers. Ainsi, après avoir procédé à l'examen de la solvabilité d'une entreprise, une agence de renseignements économiques doit être en mesure d'en communiquer les résultats à son mandant. En outre, le motif justificatif n'est opérant que si les renseignements économiques sont effectivement nécessaires à la conclusion ou à l'exécution d'un contrat. Il s'ensuit que les communications d'informations ayant trait à la solvabilité de personnes, qui ont un caractère systématique ou global, ne peuvent pas bénéficier du motif justificatif; il en va de même des réponses générales en-dehors de tout cas particulier.

La lettre d reconnaît un motif justificatif en faveur de ceux qui traitent des données en vue de leur *publication dans un média à caractère périodique*. Encore faut-il que le traitement soit effectué dans la *phase précédent* la publication. Sitôt que les données ont été publiées, les articles 28 et suivants du code civil sont applicables en lieu et place de la loi sur la protection des données (art. 2, 2^e al., let. b). La lettre d régit un domaine particulièrement controversé. Du point de vue de la protection des données, l'activité des médias, de par le grand nombre de données personnelles qu'ils brassent, n'est pas sans soulever de nombreux problèmes. Les professionnels des médias ont recours à des méthodes de collecte des données très diversifiées. Ils veulent souvent dévoiler les aspects les plus sensibles des personnes. Parfois contraints de se fonder sur des sources incertaines et de travailler contre la montre, ils ne peuvent, à ce stade, en dépit de leur conscience professionnelle, déjà garantir l'exactitude des données qu'ils traitent. Afin de disposer, à temps, de toutes les informations nécessaires lorsqu'une publication s'impose, ils rassemblent à l'avance le plus de données sensibles, les stockant généralement dans de vastes banques de données. Cela dit, on doit reconnaître qu'il ne saurait y avoir de démocratie sans média. Or, ils ne peuvent accomplir leur mission que s'ils sont en droit, d'une part, de traiter des données délicates avec une certaine marge de liberté et, d'autre part, de protéger leurs sources, du moins jusqu'à un certain point. Il s'ensuit que dans certains cas l'intérêt public au maintien de médias libres et autonomes l'emporte sur l'intérêt à la protection de la personnalité. La lettre d vise à créer un équilibre entre la protection de la personnalité et la liberté des médias. Seuls ceux qui traitent des données pour un *média à caractère périodique* peuvent invoquer le motif justificatif. Cela revient à dire que le livre et le cinéma ne sont pas protégés. Si le motif justificatif ne vaut que pour les médias périodiques, c'est parce que ceux-ci jouent un rôle essentiel dans la formation de l'opinion publique. Certes, on ne saurait nier que le livre comme le cinéma apportent également leur contribution. Reste que l'on ne peut faire bénéficier ces médias du motif justificatif sans négliger par trop les intérêts de la protection de la personnalité; en effet, il serait facile pour celui qui a commis

une atteinte à la personnalité en traitant des données de se disculper en prétendant avoir agi en vue d'une publication. En ce qui concerne la délimitation des médias qui ont un caractère périodique, nous renvoyons à la jurisprudence concernant la protection de la personnalité en droit civil (art. 28c, 3^e al., et art. 28g CC). Précisons simplement qu'entrent dans cette catégorie non seulement les produits de la presse écrite, la radio et la télévision, mais également les banques de données accessibles à tout un chacun sur appel, à condition qu'elles contiennent des données personnelles et qu'elles soient régulièrement mises à jour. Le motif justificatif couvre également la *communication* en vue d'une publication des données traitées. En effet, il ne faut pas empêcher les journalistes de soumettre à leur éditeur les projets d'articles. En outre, il importe de mettre sur le même pied les journalistes qui travaillent pour la presse écrite, la radio ou la télévision et ceux qui sont au service des agences de presse ou des agences d'images. En effet, ces agences ont pour fonction première la fourniture d'informations à des tiers, à commencer par les médias à caractère périodique.

La *lettre e* fait bénéficier d'un motif justificatif ceux qui, bien qu'ils traitent des données certes personnelles, visent un but qui est sans rapport avec les personnes concernées. Le projet privilégie expressément la *recherche*, la *planification* et les *statistiques*. Cela dit, d'autres formes de traitement dans un but ne se rapportant pas à des personnes sont envisageables; on songera, par exemple, à l'utilisation de données personnelles pour tester des équipements informatiques. La raison de ce privilège est double: d'une part la statistique, la recherche et la planification fournissent à l'économie privée des éléments de décision indispensables; d'autre part, ils répondent à de nombreux besoins sociaux et publics. Au surplus, on doit convenir que, dans le cadre de la recherche, de la planification et de la statistique, les atteintes à la personnalité, telle une violation de l'un ou l'autre des principes fondamentaux institués par l'article 4 du présent projet, sont nettement moins graves puisque ces traitements sont sans conséquence directe pour les personnes concernées. Inversement, ceux qui mènent des recherches axées directement sur des personnes ne peuvent pas invoquer ce motif justificatif. Ils peuvent en revanche – et cela concerne avant tout les historiens et les généalogistes – faire appel aux motifs justificatifs généraux institués par l'article 10, 1^{er} alinéa. Le motif justificatif spécial prévu par la *lettre e* n'entre en considération que si le résultat des recherches est publié de telle manière qu'on ne puisse en déduire des informations sur les personnes concernées. Le motif justificatif couvre également l'échange de données entre chercheurs ou entre équipes de recherche. Il faut en effet tenir compte des réalités: la recherche scientifique – et cela vaut également en partie pour la planification et la statistique – requiert une étroite collaboration entre chercheurs, parfois même au-delà des frontières; cette collaboration mérite d'être privilégiée du point de vue de la protection des données. On relèvera enfin que les diverses dispositions en vigueur sur le maintien du secret s'appliquent sans exception à la recherche, aux statistiques et à la planification. Dès lors, il est hors de question qu'un chercheur se fonde sur la *lettre e* pour justifier la communication de données secrètes.

Enfin le motif prévu à la *lettre f* peut justifier une atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun. Celui qui, par exemple dans un média, diffuse des informations, sensibles ou non, doit,

s'attendre à ce que de nombreuses personnes en prennent connaissance et le cas échéant les réutilisent. Il en va de même des opinions que quelqu'un émet en public, par exemple, lors d'une assemblée communale. Ne pas reconnaître un motif justificatif dans de tels cas équivaldrait à limiter par trop les relations sociales.

Article 11 Traitement de données par un tiers

Il n'y a aujourd'hui plus aucune difficulté d'ordre technique ou organisationnel à confier à un tiers le traitement de données. C'est là le résultat de la division du travail dans le domaine du traitement et de la communication de l'information. Dans certains cas, le traitement de l'information est, dans son intégralité, laissé au soin de spécialistes, tel un institut de sondage ou une fiduciaire. Il n'appartient pas à la loi sur la protection des données de remettre en question ce mode de procéder.

Le 1^{er} alinéa entend cependant sauvegarder les droits des personnes concernées en cas de traitement de données confiées à des tiers. Celui qui charge un tiers d'un traitement de données doit veiller à ce qu'il se conforme aux impératifs de la protection des données dans la même mesure que lui-même (let. a). Ce précepte vaut pour toutes les formes du traitement, de la collecte des données à leur communication. En confiant à un tiers le soin de traiter ses données, le mandant doit, par analogie avec l'article 55 du code des obligations, mettre tout en œuvre pour éviter d'éventuelles violations de la loi sur la protection des données. Il doit choisir soigneusement son mandataire, lui donner les instructions adéquates et le surveiller dans la mesure du possible. Suivant la lettre b, le mandant ne peut confier à un tiers le traitement lorsqu'une obligation légale ou contractuelle de garder le secret y fait obstacle. Cela signifie par exemple que le médecin qui confie à un bureau d'encaissement le traitement des factures de ses patients ne peut le faire, vu l'article 321 du code pénal, qu'avec le consentement de la personne concernée, ou il doit veiller à ce que ce bureau n'ait pas connaissance de données soumises au secret médical. Dans ce cas-ci, comme dans d'autres, les règles générales de la loi sur la protection des données s'effacent devant les règles spéciales en matière de protection des données que sont les dispositions sur le maintien du secret.

Aux termes du 2^e alinéa, le tiers peut faire valoir les mêmes motifs justificatifs que le mandant. Cette règle est nécessaire, car la personne concernée qui se prétend atteinte dans sa personnalité, peut, sur la base de l'article 28 du code civil, non seulement actionner le mandant, mais également directement le mandataire. En l'occurrence, une partie de la doctrine est d'avis, qu'à défaut des dispositions spécifiques, le mandataire n'est en droit de faire valoir que les seuls moyens dont il dispose personnellement³⁹⁾. le projet lui permet d'invoquer également les moyens de défense qui appartiennent au mandant, et ce, afin qu'en cas de litige entre la personne concernée et le mandataire, toutes les questions de protection des données puissent être tranchées dans un procès unique.

Article 12 Actions et procédure

Etant donné que la partie consacrée au droit privé de la loi sur la protection des données complète et concrétise le code civil, les règles sur la protection juridique

ne peuvent que s'aligner sur celles du droit civil. Le présent projet prévoit cependant quelques modalités particulières: il importe, d'une part, de tenir compte de certaines spécificités des traitements de données et, d'autre part, de régler les aspects de procédure de cette institution centrale du droit de la protection des données qu'est le *droit d'accès*. Conséquence de cet alignement sur le code civil: la *qualité pour agir* et la *qualité pour défendre* sont réglées de la même manière que dans le droit de la personnalité, en grande partie dans le premier cas, entièrement dans le second. Celui qui subit une atteinte illicite peut agir contre toute personne qui y participe (cf. art. 28, 1^{er} al., CC). La victime peut actionner toute personne qui aurait pu écarter l'atteinte en modifiant son comportement; elle peut de même faire constater le caractère illicite du traitement. Peu importe que le défendeur soit le principal responsable de l'atteinte ou qu'il n'y ait joué qu'un rôle accessoire⁴⁰⁾. Appliquée au traitement automatisé des données, cette règle signifie que la victime peut actionner non seulement le maître du fichier, mais aussi ses auxiliaires, son mandataire ou son serveur. Aussi peut-elle, par exemple, s'en prendre à l'exploitant d'un centre de calcul ou d'un réseau de transport de données, ou encore aux fournisseurs du logiciel ou du matériel qui ont servi au traitement illicite, pour autant que les actions ou les omissions de ces personnes aient été à l'origine de l'atteinte. Reste que la personne qui peut être appelée à répondre d'une atteinte à la personnalité n'est pas nécessairement identique à celle qui devra verser des dommages-intérêts. Les actions en dommages-intérêts sont soumises à des conditions spécifiques; le demandeur doit en particulier prouver la faute.

Enfin, on relèvera que, selon l'article premier, la loi sur la protection des données n'accorde pas la *qualité pour agir* à toutes les personnes qui ont subi une atteinte du fait d'un traitement, mais seulement à celles sur le compte desquelles des données sont traitées. Les tiers concernés n'auront dès lors la qualité pour agir que dans la mesure où le code civil la leur accorde⁴¹⁾.

Contrairement à l'avant-projet, le projet qui vous est soumis renonce à régler expressément le *droit d'action des associations*. Il s'ensuit que les règles dégagées par la jurisprudence du Tribunal fédéral dans le cadre du droit général de la personnalité sont applicables. Dès lors, une association bénéficiera de la qualité pour agir lorsqu'elle est l'objet d'une atteinte illicite imminente ou actuelle. En outre, des associations professionnelles sont en droit d'agir en leur nom, mais pour le compte de leurs membres, si la protection de la personnalité de ceux-ci relève des tâches statutaires et si ceux-ci sont eux-mêmes habilités à agir⁴²⁾.

La première phrase du 1^{er} alinéa se borne à renvoyer aux moyens de droit institués par le code civil. Trois actions différentes peuvent être intentées par la personne concernée: premièrement l'*action en interdiction*, qui permet d'empêcher une atteinte à la personnalité imminente; deuxièmement l'*action en cessation*, qui tend à mettre un terme à l'atteinte et troisièmement l'*action en constatation*, qui permet d'obtenir une reconnaissance judiciaire de l'illicéité du traitement. Conformément à la deuxième phrase de l'alinéa 1, la personne concernée peut, au moyen des actions en cessation et en interdiction, en particulier requérir la *rectification* ou la *destruction des données*. Ce sera là certainement les deux demandes les plus courantes en matière de protection des données. Suivant l'article 28c du code civil,

la personne concernée pourra également requérir des *mesures provisionnelles*. A cet effet, elle n'aura qu'à rendre vraisemblable qu'elle est l'objet d'une atteinte illicite à la personnalité.

Le 2^e *alinéa* institue un moyen de droit particulier: la possibilité de faire mentionner le *caractère litigieux* d'une donnée. Il est en effet très souvent difficile de prouver l'exactitude ou l'inexactitude de faits liés avant tout à un jugement de valeur. Il importe alors que la personne concernée soit en droit de demander que l'on ajoute aux données la mention de leur caractère litigieux. De cette façon, elle peut donner son avis sur une information sans avoir à passer par la voie limitée et dès lors plus difficile et incertaine de l'action en rectification ou en destruction. Il appartiendra à la jurisprudence de déterminer à quelles conditions concrètes il pourra être fait droit à une requête en mention du caractère litigieux. Le juge tiendra compte des circonstances et de ce qu'on peut raisonnablement exiger de la personne qui traite les données pour fixer l'étendue et la teneur de la mention. Relevons enfin qu'une requête en mention du caractère litigieux peut également être introduite par la voie des mesures provisionnelles au sens de l'article 28c du code civil.

Le 3^e *alinéa* dispose que les actions en exécution du *droit d'accès* doivent être ouvertes au même for que celui que l'article 28b du code civil prévoit pour les actions en protection de la personnalité en général. Le 3^e *alinéa* impose en outre une procédure simple et rapide, au motif notamment que du sort de l'action en exécution du droit d'accès dépend l'ouverture ou non d'une action en protection de la personnalité. A l'instar de l'article 28b, 1^{er} *alinéa*, du code civil, la concrétisation du droit matériel implique ici aussi la mise en place de normes de procédure fédérale.

221.4 Section 4: **Traitement de données personnelles par des organes fédéraux**

Article 13 Organe responsable

Pour accomplir leurs différentes tâches légales, les autorités et les services administratifs, quelquefois également des particuliers et des organisations privées, traitent un très grand nombre de données personnelles. Dès lors, le 1^{er} *alinéa* prévoit que chacun de ces organes fédéraux doit, dans les limites de ses attributions légales et réglementaires, assumer les responsabilités qui lui incombent au titre du droit de la protection des données. C'est à eux qu'il incombe notamment de donner accès aux fichiers, de respecter les règles sur la communication des données et de prendre les mesures de sécurité qui s'imposent. Il importe d'attribuer la responsabilité pour les traitements de données directement aux services qui sont appelés à appliquer les prescriptions sur la protection des données, et non à la Confédération en tant que telle ou au Conseil fédéral en tant qu'autorité directrice de l'administration. Etant donné que la législation sur l'organisation de la Confédération ne définit, en règle générale, que les tâches des *offices*, il ne sera pas toujours aisé de déterminer concrètement sur quelle unité administrative repose la responsabilité. Selon les cas, il se pourra que la responsabilité pour certains traitements de données soit attribuée à des unités ad-

ministérielles de rang inférieur, telle la division ou la section. En définitive il appartient aux départements ou aux offices de répartir les responsabilités, et ce, de manière transparente pour les administrés. A cet égard, on relèvera que le registre des fichiers contenant des données personnelles, récemment publié par l'Office fédéral de la justice, désigne l'organe responsable de chaque fichier.

Le 2^e alinéa attribue au Conseil fédéral la compétence de réglementer les responsabilités de manière spécifique à chaque fois qu'un des organes fédéraux traite des données conjointement avec d'autres organes fédéraux ou avec des organes cantonaux ou encore avec des personnes privées. Cette disposition vise surtout les grands systèmes décentralisés d'informations et les systèmes dits «répartis». On entend par *systèmes décentralisés*, les systèmes informatiques dans lesquels la saisie des données est effectuée non par l'exploitant du système lui-même, mais par des participants situés à la périphérie. Tel est le cas du système PERIBU (système d'informations concernant le personnel de l'administration fédérale); si ce système est géré par l'Office du personnel, les données sont en revanche introduites directement par les services du personnel des différents offices. Par *systèmes «répartis»*, on entend les systèmes obtenus par l'interconnexion de plusieurs ordinateurs indépendants; avec le développement toujours plus grand des ordinateurs personnels ces systèmes vont connaître un succès grandissant. Les systèmes conjointement gérés par la Confédération et les cantons risquent de poser des problèmes de responsabilité particulièrement délicats. Une solution raisonnable de ces problèmes passe, en partie du moins, par une réglementation fédérale. Il s'agira avant tout d'attribuer la responsabilité du système – principale ou en dernier ressort – à un organe déterminé. En outre, il faudra établir dans quelle mesure chaque participant aura le droit de consulter les données contenues dans le système et devra veiller à leur exactitude et à leur sécurité. Enfin, il faudra régler, dans le détail, les modalités d'accès des personnes concernées à leurs propres données. Le Conseil fédéral est également en droit de subdéléguer la responsabilité aux départements, lorsque tous les participants au système relèvent d'un seul et même département.

Article 14 Bases juridiques

Le 1^{er} alinéa dispose que, à l'instar de toute activité administrative effectuée par un organe fédéral, tout traitement de données nécessite une base légale. Cette règle est applicable à toutes les formes et à tous les stades du traitement de données, à moins que l'un des articles qui suivent ne contienne une exception expresse. Par base juridique, on entend soit un traité international, soit une disposition de rang constitutionnel ou légal, soit encore une disposition de rang réglementaire, fondée sur l'un de ces actes. Le degré de précision de la base juridique s'appréciera d'après les principes généraux en la matière. Différents critères peuvent ainsi entrer en considération; parmi ceux-ci, on relèvera la gravité de l'atteinte aux libertés de l'administré, la nature des données traitées, le cercle des personnes concernées, la structure du système informatique ou, le cas échéant, la participation de services cantonaux ou de personnes privées au traitement. A tout le moins, la base juridique doit définir le but du traitement, décrire, dans les grandes lignes, son importance, et désigner les organes qui y participent. Toutefois, étant donné la variété presque infinie des modes de

traitement au sein de l'administration fédérale, la base juridique ne doit pas recevoir une interprétation trop étroite. Il suffira que le traitement d'informations soit en relation évidente avec les tâches de l'organe fédéral concerné. Au demeurant et sauf disposition légale contraire, les organes fédéraux ne doivent procéder à des traitements de données qu'en conformité avec les principes posés par l'article 4.

Le 2^e alinéa soumet le traitement de *données personnelles sensibles* et de *profils de la personnalité* à un régime juridique plus sévère. Ainsi, la lettre a exige que le traitement soit prévu dans une *loi au sens formel*, notion qui englobe aussi les traités internationaux et les arrêtés de portée générale. Toutefois, force est de constater qu'il ne sera guère possible de créer pour chaque traitement de données sensibles la base légale nécessaire; c'est pourquoi on doit également tolérer le traitement lorsqu'il n'y a aucun doute que l'accomplissement d'une tâche légale clairement définie l'exige (let. b). En revanche, le simple fait que le recours à des données sensibles ou à des profils de la personnalité puisse faciliter l'exécution de cette tâche n'est pas en soi suffisant. Au surplus, le Conseil fédéral doit, dans un cas particulier, être en mesure d'autoriser le traitement de données sensibles ou de profils de la personnalité s'il s'avère nécessaire de parer au plus pressé. Encore faut-il qu'il soit convaincu que les droits de la personne concernée ne sont pas menacés (let. c). Enfin, il est toujours possible de traiter des données sensibles ou des profils de la personnalité si la personne concernée y a consenti ou a rendu ses données accessibles à tout un chacun (let. d). Reste que la personne concernée doit avoir donné son consentement en connaissance de cause; il ne saurait y avoir de consentement global: la personne concernée doit avoir donné son consentement dans chaque cas d'espèce. En ce qui concerne la seconde condition de la lettre d, nous vous renvoyons à nos commentaires concernant l'article 10, 2^e alinéa, lettre f. Les traitements effectués en conformité aux lettres c et d doivent, pour le moins, reposer sur une base légale au sens du 1^{er} alinéa.

Article 15 Collecte de données personnelles

Les prescriptions spéciales sur la collecte de données personnelles *complètent*, d'une part, les principes fondamentaux énoncés à l'article 4 et, d'autre part, les prescriptions générales applicables au traitement posées par l'article 14. A l'heure où l'administration requiert toujours plus d'informations personnelles, il importe de veiller à ce que celles-ci soient collectées de telle manière que la personne concernée puisse prendre position et le cas échéant s'opposer à un traitement illicite.

A cet effet, le 1^{er} alinéa prévoit que les données doivent être collectées de manière reconnaissable pour la personne concernée. On ne peut mieux respecter ce principe qu'en collectant les données *directement auprès de la personne concernée*. Cela dit, la collecte de données auprès de tiers est parfaitement admissible, à condition que la personne concernée en soit consciente. En effet, la collecte des données auprès des ceux qui les détiennent déjà est, pour l'administration, une solution rationnelle qu'il n'y a pas lieu de remettre fondamentalement en question. L'administré a également tout à gagner à ce que chaque service de l'administration ne vienne pas l'importuner en collectant chacun les mêmes données.

Etant donné que la collecte systématique de données, notamment au moyen de *questionnaires* permet de rassembler une grande quantité de données, le 2^e *alinéa* impose à l'organe responsable l'*obligation particulière* d'informer la personne concernée. On relèvera que, même si les données ne sont pas conservées dans un fichier, la personne concernée obtiendra les mêmes informations que pour un fichier (cf. art. 5).

Enfin, sur la base du 3^e *alinéa*, il est loisible de renoncer à informer la personne concernée du traitement dans trois cas: lorsque celle-ci a rendu ses données accessibles à tout un chacun, par exemple dans un livre (let. a); lorsque l'accomplissement de la tâche de l'organe fédéral en serait compromise (let. b) ou lorsqu'il en résulterait un volume excessif de travail (let. c). On songe notamment aux relevés de statistiques.

Article 16 Communication de données personnelles

L'expérience le montre à l'envi: la réglementation sur la communication des données personnelles tient une place prépondérante dans toute législation de droit public sur la protection de la personnalité. A l'origine de la présente disposition, il y a la constatation que l'Etat moderne a toujours plus recours aux traitements de données. Ceux-ci sont au centre d'un conflit entre les nécessités d'une administration coordonnée et rationnelle d'une part, et les impératifs de la protection de la personnalité d'autre part. S'il est certes incontestable que les unités administratives doivent collaborer à l'exécution de tâches communes, on doit cependant reconnaître qu'il n'y a pas lieu de leur donner le droit d'accéder à leur guise à l'ensemble des données traitées par l'appareil étatique. Il est indispensable d'instituer un certain cloisonnement entre les unités administratives, autrement dit une séparation des ressources en informatique.

Toutefois notre ordre juridique ne contient actuellement que quelques dispositions ponctuelles sur l'échange d'informations entre les services administratifs. Ainsi, selon la plupart des législations sur le statut des fonctionnaires, le secret de fonction interdit entre autre à un fonctionnaire de révéler à une autre autorité des informations qui doivent être tenues secrètes⁴³). A l'inverse, en vertu des dispositions sur l'entraide administrative et judiciaire, il peut incomber aux autorités une obligation de donner des informations. Ces dispositions sont néanmoins rares⁴⁴); mis à part quelques arrêts isolés concernant l'entraide judiciaire en matière pénale⁴⁵), la jurisprudence n'a pas encore dégagé les principes fondamentaux de l'entraide judiciaire et administrative en droit suisse. Le présent article continue dès lors en quelque sorte une *disposition générale sur l'entraide administrative et judiciaire* et une *disposition d'exécution du secret général de fonction*. En effet, il détermine à quelles conditions les organes fédéraux peuvent communiquer des données personnelles. Cependant, il n'institue *aucune obligation* de communiquer des données; même si toutes les conditions définies à l'article 16 sont remplies, l'organe compétent doit examiner encore si la communication envisagée est en tous points conforme aux principes posés par l'article 4. En conséquence, il est hors de question, par exemple, de communiquer des données à l'étranger si la personnalité des personnes concernées s'en trouvait gravement menacée (cf. art. 4, 5^e al.). Les règles sur la communication des données valent aussi bien pour les échanges d'informations entre organes fédéraux que pour la

communication à des autorités cantonales, communales ou étrangères, voire encore à des personnes privées domiciliées en Suisse ou à l'étranger. Elles sont un complément à l'article 14.

Le 1^{er} alinéa n'autorise la communication que dans cinq cas:

Des données peuvent être communiquées s'il existe une *base juridique* à cet effet, c'est-à-dire une loi, une ordonnance ou un traité. Cette base doit prévoir expressément le *transfert des données*. En conséquence, une simple compétence générale pour traiter les données, au sens de l'article 14, est insuffisante. En revanche, il n'y a pas lieu de se demander si l'autorité qui communique les données exerce un droit ou s'acquitte d'une obligation, ou encore fait droit à une prétention du destinataire des données.

A défaut de base juridique, des données personnelles peuvent être communiquées si le destinataire a en l'espèce besoin de ces données pour accomplir sa tâche légale (let. a). La restriction aux cas d'espèces implique qu'il ne saurait y avoir de consultation permanente d'un fichier sans base juridique; partant, sont bannis et l'accès en ligne et la fourniture systématique de listes. Par cas d'espèce au sens de la lettre a, on entend la communication de données à une finalité unique. Peu importe qu'il s'agisse de données relatives à une *personne particulière ou concernant plusieurs personnes*.

L'absence de base juridique peut être palliée par le consentement – exprès ou tacite – de la personne concernée (let. b). Cela dit, le consentement doit viser le cas d'espèce; on ne saurait admettre de consentement global. Cela ne signifie pas pour autant que seul le consentement donné à propos d'une communication unique est valable. La personne concernée peut aussi donner son consentement pour plusieurs communications du moment que les circonstances dans lesquelles elles interviennent lui sont claires. Il est ainsi tout à fait concevable qu'un employé autorise son employeur, une fois pour toutes, à renseigner d'éventuels employeurs sur ses qualifications (cf. aussi le nouvel art. 328b CO proposé, ch. 221.1). Relevons en outre que s'il est impossible ou difficile de requérir l'accord de la personne concernée, il suffira que les circonstances permettent de présumer que la personne aurait approuvé la communication.

La communication de données est aussi permise lorsque la personne concernée a de toute façon déjà rendu ses données publiques, par exemple en les publiant dans un livre ou un journal (let. c).

On relèvera finalement que la communication de données en l'absence de base juridique ou du consentement de la personne concernée est possible dans un cas: lorsque la personne concernée s'oppose à la communication de manière abusive (let. d). Cette disposition devrait trouver son application pratique surtout dans le domaine des prétentions découlant du droit de la famille; un exemple concret: le parent ou l'enfant bénéficiaire d'une pension alimentaire s'adresse à l'ambassade de Suisse dans le pays où s'est établi l'autre parent afin de connaître son adresse. Cette disposition n'est pas sans signification dans le domaine des assurances sociales; que l'on songe à un employé qui veut savoir si son employeur a versé les cotisations le concernant. Par analogie avec le droit d'être entendu, la personne concernée sera, dans la mesure du possible, invitée à se prononcer préalablement à la communication. Ce «droit d'être entendu» n'a cependant aucun caractère

abolu; l'organe fédéral peut renoncer à prendre l'avis de la personne concernée dans deux cas; premièrement, lorsque des prétentions juridiques ou des intérêts légitimes de tiers risquent d'être compromis; deuxièmement, lorsque la personne concernée n'est pas atteignable ou ne s'est pas prononcée dans le délai imparti.

La communication de données sensibles ou de profils de la personnalité est, à l'instar de leur traitement, soumise à un régime juridique particulier. A moins que la personne concernée ait consenti à la communication ou ait rendu ses données publiques, la communication doit être expressément prévue par une loi ou être indispensable à l'accomplissement d'une tâche clairement définie dans un texte légal. Si ces conditions ne sont pas réunies, il y a toujours la possibilité de solliciter une autorisation du Conseil fédéral (cf. art. 14, 2^e al.).

Suivant le 2^e alinéa, les organes fédéraux sont en droit de communiquer, à la demande d'un autre organe ou d'un particulier, le nom et le prénom, l'adresse et la date de naissance d'une personne. Cette possibilité répond à un vœu maintes fois exprimé lors de la procédure de consultation. Il importe de faciliter la communication de certaines données, plus ou moins connues, permettant d'identifier une personne. Le 2^e alinéa ne *contraint* cependant pas les organes fédéraux à communiquer ces données: il leur appartient en fin de compte de prendre en considération, à chaque fois, le besoin de protection de la personne concernée. Ainsi y a-t-il lieu de refuser l'octroi de ces informations, lorsque l'on peut tirer des conclusions péjoratives sur la personne concernée du simple fait que tel ou tel organe possède ses coordonnées. A titre d'exemple, on citera le cas des autorités de poursuite pénale de la Confédération. Au besoin, il appartiendra au Conseil fédéral de désigner nommément les services administratifs habilités à donner les informations prévues au 2^e alinéa.

Le 3^e alinéa spécifie dans quels cas un organe fédéral peut ou doit restreindre une communication pourtant autorisée par la loi. L'existence d'un *important intérêt public* ou d'un *intérêt légitime manifeste* de la personne concernée constitue le premier cas (let. a). Il s'agit là d'une sorte de réserve d'ordre public, qui est valable à l'encontre de n'importe quel destinataire. Par important intérêt public, on entend avant tout la protection de l'Etat et la sécurité militaire. Quant à l'expression «intérêt légitime manifeste de la personne concernée», elle vise par exemple, la nécessité d'occulter l'identité d'une personne impliquée dans une enquête administrative. En outre, la lettre b réserve les *obligations légales de garder le secret ou une des dispositions particulières de protection des données*. Certains domaines, notamment celui des assurances sociales, connaissent des obligations spéciales de garder le secret; celles-ci n'autorisent la communication de données personnelles que dans des cas exceptionnels, expressément spécifiés par le Conseil fédéral⁴⁶⁾. De même, il existe déjà un certain nombre de dispositions de protection des données valables pour des domaines particuliers; celles-ci déterminent le cercle des destinataires des données et, quelquefois même, la nature des données qui peuvent être transmises⁴⁷⁾. Ces dispositions doivent être considérées comme des normes spéciales au sens de l'article 16 du projet.

La teneur des dispositions sur la communication des données – ajoutées aux dispositions sur la collecte des données – rendent inutile toute réglementation spécifique de la *communication des données aux autorités fiscales*. La pratique

suivie jusqu'à aujourd'hui en matière de communication d'informations aux autorités fiscales peut être maintenue pour l'essentiel. La plupart des lois fiscales prévoient des obligations expresses d'entraide administrative⁴⁸⁾; ce faisant, la base juridique nécessaire à la communication de données, parfois même de données sensibles, est établie. A défaut d'une telle base légale, les autorités fiscales, se fondant sur l'article 16, 1^{er} alinéa, lettre a, peuvent toujours obtenir les renseignements souhaités dans un cas particulier; encore faut-il que ces informations soient absolument nécessaires à l'accomplissement de leurs tâches. Tant que cette dernière condition est strictement respectée, cette manière de faire ne viole pas le principe de la compatibilité des buts posé à l'article 4, 4^e alinéa. Suivant l'article 15 du projet, les autorités fiscales sont néanmoins tenues d'informer la personne concernée dans ces cas à chaque fois qu'elles ne collectent pas directement les données auprès d'elle. L'obligation de renseigner les autorités fiscales se justifie au demeurant entièrement car ces dernières sont soumises au secret fiscal; celui-ci est un devoir de discrétion qualifié que les autorités fiscales ont à l'égard aussi bien des personnes privées que des autres autorités.

Article 17 Blocage des données

Cette disposition accorde à la personne concernée le *droit – limité – de s'opposer* à une communication de données personnelles pourtant licite. Cette possibilité de blocage prend toute sa signification en cas de communication de données à l'étranger ou à des personnes privées, soit dans des cas où l'organe responsable n'est pas à même d'apprécier l'ensemble des dangers que pourrait faire encourir la communication. Il importe dès lors de donner à la personne concernée la possibilité de défendre aussitôt ses intérêts. Il est également possible de bloquer une communication de données entre autorités; toutefois, cette possibilité devrait rarement entrer en ligne de compte, car dans la plupart des cas la clause d'exception instituée par le 2^e alinéa sera applicable. Le droit au blocage ne peut s'exercer de manière globale: s'adressant aux organes compétents, la personne concernée doit à chaque fois désigner précisément les données visées.

Suivant le 1^{er} alinéa le droit au blocage n'appartient pas à n'importe quelle personne concernée, mais seulement à celle qui rend vraisemblable un intérêt légitime. Légitime, l'intérêt de la personne concernée qui affirme que les destinataires des données lui font subir des tracasseries ou des pressions, voire même des persécutions, l'est assurément.

Au demeurant, le 2^e alinéa restreint les effets du blocage. Ainsi, cette disposition contraint l'organe responsable à communiquer les données nonobstant le blocage, lorsqu'une obligation juridique impose la communication des données (let. a) ou, lorsque le défaut de communication viendrait à compromettre l'accomplissement de ses tâches (let. b).

Article 18 Obligation de rendre les données personnelles anonymes ou de les détruire

Les procédés modernes de copie des informations, de même que les mesures de sécurité nécessitées par les traitements automatisés des données, ont conduit à la constitution de vastes stocks de données. Si nombre de ces copies perdent rapidement tout intérêt pratique, elles comportent en revanche certains risques

+ d'atteinte à la personnalité. L'article 18 dispose dès lors que ces données doivent être détruites, ou, à tout le moins, rendues anonymes. Cette obligation découle directement du principe de proportionnalité tel que l'article 4, 3^e alinéa, du présent projet le conçoit dans le cadre du traitement de données. Cependant, l'article 18 n'impose pas la destruction ou l'anonymisation de toutes les données qui ne sont plus nécessaires aux activités administratives ordinaires. En effet, certaines données doivent être conservées à titre de preuve, par mesure de sûreté ou encore en vue d'une éventuelle demande de révision (let. a). Il en va de même, suivant la lettre b, des documents qui doivent être versés aux Archives fédérales en vertu du règlement y relatif; il s'agit avant tout des documents qui ont une valeur historique. On relèvera enfin que les dispositions du règlement des Archives fédérales doivent être considérées comme des normes spéciales qui priment l'article 18 du présent projet.

Contrairement à l'avant-projet, nous avons renoncé à réglementer l'*archivage des données*. Le projet qui vous est soumis (cf. art. 3, let. g) entend par «documents déposés aux archives», les documents conservés à l'écart des dossiers courants, qui sont plus difficilement consultables, soit du fait de mesures organisationnelles, soit du fait de leur éloignement. On songe en particulier aux documents qui sont conservés sous clé, et, partant, qui ne sont accessibles qu'à certaines personnes déterminées, ou encore aux informations conservées sur un support électronique qui ne peuvent être consultées qu'au moyen d'un code d'accès spécial. Par un archivage adéquat, on peut respecter la plupart des exigences posées par la protection des données. Cependant, il est impossible d'édicter des règles générales susceptibles d'appréhender les divers aspects pratiques de l'archivage. Il y a en effet autant de méthodes d'archivage que de services administratifs fédéraux ou d'organismes appelés à exécuter des tâches fédérales. A quoi s'ajoute une appréciation souvent fort différente des données utilisées continuellement, occasionnellement ou exceptionnellement. Il s'ensuit qu'il est nécessaire d'édicter pour chaque domaine sa réglementation spécifique.

Article 19 Traitement aux fins de recherche, de planification et de statistique

La réglementation spéciale instituée par l'article 19 se justifie à un double titre: d'abord l'intérêt public à la recherche, à la planification et à la statistique; ensuite, le fait que les traitements de données effectués à ces occasions sont moins dangereux pour la personnalité, car ils ne se rapportent pas à des personnes. De ce fait, l'article 19 prévoit plusieurs dérogations aux principes généraux posés par le présent projet. Cette disposition vise deux situations: premièrement, celle où l'organe responsable traite les données qu'il détient à des fins ne se rapportant pas à des personnes; deuxièmement, celle où il communique les données à des organes de la Confédération ou des cantons, ou encore à des personnes privées, à des fins de recherche, de planification ou de statistique. Dans ce cas cependant les obligations particulières de garder le secret sont réservées.

Le 1^{er} alinéa énonce à quelles conditions un organe fédéral peut invoquer le privilège de la recherche; ces conditions sont cumulatives. Première condition: l'organe qui utilise des données personnelles à des fins de recherche, de planification ou de statistique, doit les rendre anonymes aussitôt que le traitement le permet (let. a). On entend par rendre anonyme, toute démarche visant à

empêcher l'identification des personnes concernées ou à ne rendre celle-ci possible qu'au prix d'efforts démesurés. En pratique, il arrive fréquemment que le chercheur, le planificateur ou le statisticien, bien qu'il utilise des données dépourvues de références à des personnes déterminées, n'entende néanmoins pas les rendre d'emblée anonymes, car il doit conserver la possibilité de vérifier exceptionnellement l'identité d'une personne. Lorsqu'il est confronté à de telles situations, il se doit de coder ou de crypter les données. Il peut, par exemple, séparer les caractéristiques personnelles des autres données, de telle sorte qu'il ne soit plus possible de mettre en relation telle donnée avec telle personne sans passer par le numéro de référence. Cette manière de procéder est aujourd'hui déjà fort courante. A chaque fois qu'il communique des données à des fins de recherche, de planification ou de statistique, l'organe fédéral doit s'assurer, au moyen de charges instituées par contrat ou par instruction, que le destinataire des données ne transmette à son tour les données à des tiers qu'avec son consentement (let. b). Il importe en effet de veiller à ce que ce tiers ne réutilise les données qu'à des fins de recherche, de planification ou de statistique, ou à tout autre fin ne se rapportant pas à des personnes. Enfin, les privilèges institués par l'article 19 sont liés à la condition que les résultats du traitement soient publiés sous une forme ne permettant pas, selon le cours ordinaire des choses, d'identifier les personnes concernées (let. c).

Le 2^e alinéa énumère exhaustivement les dispositions de la loi qui ne sont pas applicables au traitement de données ne se rapportant pas à des personnes. Il s'agit d'abord du principe de la compatibilité des buts institué par l'article 4, 4^e alinéa. Etant donné que la recherche, la planification ou la statistique sont des activités sans effet direct sur les personnes concernées, il n'y a pas lieu d'interdire l'utilisation de données qui ont été collectées à de toutes autres fins (let. a). Pour la même raison, les organes fédéraux pourront traiter des données sensibles ou des profils de la personnalité – encore que cette dernière éventualité n'aura en pratique qu'un rôle mineur – à des fins de statistique, de recherche ou de planification, ou encore à tout autre fin ne se rapportant pas à des personnes, sans être tenus de se conformer aux conditions spéciales instituées par l'article 14, 2^e alinéa, (let. b) pour autant que l'exigence d'une base juridique, posée par l'article 14, 1^{er} alinéa, soit respectée. Il n'est pas nécessaire non plus qu'ils observent les dispositions générales sur la communication de données (let. c). Il s'ensuit que la communication de données à des fins ne se rapportant pas à des personnes ne nécessite aucune base juridique supplémentaire. Il n'est pas non plus exigé que le destinataire ait absolument besoin des données pour accomplir une tâche légale, ni que la personne concernée ait donné son consentement. Cela dit, en vertu du 1^{er} alinéa, lettre b, l'organe fédéral qui a collecté les données doit donner son accord à leur nouvelle transmission.

Article 20 Activités de droit privé des organes fédéraux

Du fait de leurs activités commerciales, certains services administratifs de la Confédération, notamment les CFF, les PTT et les centrales d'achats de l'administration fédérale sont confrontés à la concurrence économique. Le 1^{er} alinéa dispose qu'ils doivent être mis sur le même pied que leurs concurrents lorsqu'ils agissent selon le droit privé, autrement dit lorsqu'ils ne sont pas investis de

prérogatives de puissance publique. Cette situation se caractérise par le fait que les relations avec les tiers ne prennent pas la forme de décisions mais d'accords de droit privé. A ces conditions, il importe de faire bénéficier ces services administratifs du régime moins sévère applicable aux personnes privées (cf. sect. 3). Concrètement, cela signifie que, par exemple, ils sont en droit de rejeter une demande d'accès au simple motif qu'ils sont en concurrence économique (art. 6, 1^{er} al., let. d); les règles de cette section concernant le traitement ne sont pas applicables.

Le privilège dont bénéficie un organe fédéral qui, agissant selon le droit privé, est confronté à la concurrence économique ne s'étend pas, suivant le 2^e alinéa à la *réglementation sur la surveillance*. Le préposé à la protection des données est en effet en droit d'exercer son contrôle sur les activités de droit privé de l'organe fédéral dans la même mesure que sur ses activités découlant de prérogatives de puissance publique. Cela signifie que les organes fédéraux en concurrence économique ont les mêmes devoirs d'enregistrement et de déclaration (art. 7 et 8) que les autres organes fédéraux.

Article 21 Protection de l'Etat et sécurité militaire

Les organes de protection de l'Etat et de sécurité militaire – en particulier la police fédérale et les services de renseignements et de sécurité militaires –, ne peuvent pas exécuter leurs tâches sans traiter un grand nombre de données personnelles. Leurs informations, ils sont contraints de les rechercher auprès de diverses sources. Le traitement de ces informations requiert le plus grand secret; il importe notamment de protéger les collaborateurs de ces services. D'un autre côté, une certaine collaboration avec les services chargés de la protection de l'Etat et de la sécurité militaire de pays étrangers est indispensable. De ce fait, il est difficile d'établir des règles générales concernant les traitements de données effectués par des services chargés de la protection de l'Etat. La nécessité de promouvoir une protection des données efficace est dans ce domaine manifeste; et vu que les intérêts supérieurs de l'Etat sont en jeu, cette protection ne peut être que limitée. Il s'ensuit que l'article 21 attribue au Conseil fédéral la compétence de déroger aux règles générales de la loi sur la protection des données en faveur des services chargés de la protection de l'Etat et de la sécurité militaire. Le Conseil fédéral peut prévoir ces dérogations soit par la voie réglementaire, soit par la voie d'autorisations spéciales.

Le 1^{er} alinéa énumère exhaustivement les dispositions de la présente loi auxquelles il peut être dérogé. Ainsi, le Conseil fédéral pourra autoriser les organes de protection de l'Etat et de sécurité militaire à ne pas se conformer aux principes de la compatibilité des buts (art. 4, 4^e al.) et aux exigences mises à la communication de données à l'étranger (art. 4, 5^e al., let. a). C'est le propre des services de protection de l'Etat d'opérer au moyen de données qui n'ont pas été collectées à l'origine à cette fin. Eu égard aux intérêts supérieurs de l'Etat, les échanges d'informations avec des services étrangers de protection de l'Etat doivent pouvoir s'effectuer même si d'éventuels inconvénients pour la personne concernée ne sont pas exclus. Il importe que les échanges d'informations, dans l'intérêt de la sûreté intérieure et extérieure, avec les autorités étrangères – échanges d'informations qui se font aujourd'hui sur la base de l'arrêté du Conseil fédéral sur le service de

police du Ministère public de la Confédération, ainsi que sur la base des prescriptions du Département fédéral de justice et police y relatives⁴⁹⁾ – puissent à l'avenir se poursuivre dans les mêmes proportions; partant, il est nécessaire de déroger à l'article 4, 5^e alinéa. En outre, les autorités de protection de l'Etat peuvent rarement se passer de données sensibles. Dès lors, le Conseil fédéral doit être habilité à autoriser le traitement de telles données, alors même que les conditions spéciales posées par la loi sur la protection des données ne sont pas remplies (let. b). Maintien du secret oblige, les autorités de protection de l'Etat doivent au surplus être libérées, à certaines conditions, de l'obligation d'annoncer au préposé à la protection des données les fichiers et les communications de données à l'étranger (let. c). Cela dit, le Conseil fédéral peut maintenir l'obligation d'annoncer un fichier au préposé à la protection des données, tout en prescrivant que le fichier ne sera pas publié au registre des fichiers. Enfin, le Conseil fédéral doit être en mesure de régler la coopération entre les autorités de protection de l'Etat et de la sécurité militaire d'une part et le préposé à la protection des données d'autre part, en dérogation aux principes généraux de la loi (let. d). Il s'agira avant tout de déterminer dans quelle mesure le préposé à la protection des données conservera le droit de demander des informations et de consulter des pièces (cf. art. 24, 3^e al.).

Le 2^e alinéa rappelle que ni le secret de vote, ni le secret de pétition, ni le secret des statistiques ne saurait être violé au profit de la protection de l'Etat ou de la sécurité militaire.

S'agissant des affaires relevant de la protection de l'Etat, il importe que le cercle des détenteurs d'un secret demeure le plus restreint possible; à cet effet, le 3^e alinéa prévoit qu'il appartiendra au département dont relève l'organe concerné (DFJP ou DMF), et non à la Commission fédérale de la protection des données – respectivement à son président – de se prononcer sur les différends entre les services de protection de l'Etat d'une part et le préposé et la personne concernée de l'autre; celle-ci pourra, le cas échéant, porter la décision du département devant le Conseil fédéral. Quant aux différends entre le préposé à la protection des données et les services chargés de la protection de l'Etat, ils sont directement tranchés par le Conseil fédéral. Ces voies de droit sont conformes à la réglementation générale de la procédure fédérale applicable aux affaires relevant de la protection de l'Etat (art. 100, let. a, OJ; RS 173.110).

Article 22 Prétentions et procédure

Il n'y a pas seulement un intérêt public à ce que les organes fédéraux traitent les données personnelles conformément aux prescriptions de la loi, mais également un intérêt privé: celui de chaque personne concernée. L'article 22 lui donne les *moyens juridiques* d'exiger que les traitements de données soient effectués conformément à la loi. En outre, il règle la procédure que devra suivre la personne concernée pour faire valoir ses exigences. La réglementation proposée se fonde, d'une part, sur les actions de droit privé instituées par l'article 12 du présent projet et l'article 28a du code civil et, d'autre part, sur la procédure administrative en vigueur.

Suivant le 1^{er} alinéa seul celui qui bénéficie d'un *intérêt légitime* peut faire valoir, à l'encontre de l'organe responsable, les prétentions juridiques qui découlent du

droit de la protection des données. La jurisprudence administrative met au bénéfice d'un intérêt légitime non seulement la personne concernée mais également, à certaines conditions, un tiers dont les données personnelles ne sont pas en cause. La qualité pour agir est ainsi accordée à un cercle de personnes plus large que celui prévu dans la partie de la loi consacrée au droit privé; on relèvera cependant que des tiers peuvent, dans certaines conditions, s'en prendre à des traitements de données qui ne concernent pas directement leur propre personne, en se fondant sur la protection générale de la personnalité instituée par le code civil. Quant à la qualité pour agir des *associations*, elle est définie par les principes généraux du droit administratif. Il s'ensuit que les associations peuvent faire valoir les prétentions qui découlent du droit de la protection des données à condition qu'elles justifient d'un *intérêt propre*; elles sont également habilitées à *faire valoir les intérêts d'un de leurs membres* à la double condition, d'abord que la défense des intérêts d'une majorité ou d'une grande partie de leurs membres relève de leurs tâches statutaires, ensuite que les membres aient qualité pour faire valoir individuellement la même prétention⁵⁰). A l'instar de la partie que la loi consacre au droit privé, les requêtes peuvent tendre à ce qu'on s'*abstienne de procéder* à un traitement illicite (let. a), à ce que les *effets* d'un traitement illicite soient *supprimés* (let. b) ou à ce que le *caractère illicite* du traitement soit *constaté* (let. c). Comme nous l'avons déjà dit (cf. nos remarques concernant l'art. 5), le droit d'accès aux dossiers qui découle de l'article 4 de la constitution permet, à certaines conditions, d'obtenir la *source* d'une donnée; quant à d'éventuelles prétentions en dommages-intérêts, elles sont régies par la loi sur la responsabilité de la Confédération.

Le 2^e alinéa précise qu'il est possible de demander une *rectification* ou une *destruction* des données par la voie des actions en cessation et en suppression du trouble (let. a). En outre, il prévoit, à l'instar de l'article 28a, 2^e alinéa, du code civil, la possibilité de publier ou de communiquer à des tiers la décision (p. ex. la constatation qu'un traitement était illicite ou la rectification d'une donnée; let. b).

Le 3^e alinéa étend au secteur public la possibilité de faire *mentionner le caractère litigieux* d'une donnée. Cet alinéa introduit une disposition spéciale sur le *fardeau de la preuve*. En droit administratif, la maxime officielle est de rigueur; dès lors, un organe fédéral qui est saisi d'une requête fondée sur le droit de la protection des données doit d'office élucider les faits. Les parties sont tenues toutefois de collaborer à l'établissement de ceux-ci. Si l'enquête administrative ne permet pas d'établir l'exactitude ou l'inexactitude d'une donnée et si l'organe refuse de renoncer à la donnée litigieuse, il reste la possibilité d'ajouter à la donnée la mention de son caractère litigieux. Cette mention est le signe que la personne concernée ne partage pas l'avis des autorités sur la présentation des faits. Sous quelle forme la mention sera-t-elle ajoutée: simple signe distinctif ou plutôt genre droit de réponse? Il appartiendra à la jurisprudence de l'établir.

Le 4^e alinéa prévoit expressément que les requêtes fondées sur l'article 22 doivent être traitées suivant les règles de la loi fédérale sur la procédure administrative. Cela vaut aussi pour les domaines qui échappent au champ d'application de cette loi en vertu de ses articles 2 et 3. En effet, les raisons qui ont motivé ces exceptions – notamment l'existence de dispositions spéciales de procédure ou la nécessité de prendre une décision rapidement – sont dépourvues de toute pertinence en

protection des données. L'applicabilité de la loi fédérale sur la procédure administrative implique avant tout que les requêtes découlant des 1^{er} et 2^e alinéas de l'article 22 doivent nécessairement faire l'objet d'une *décision*. Il appartiendra à l'autorité compétente de déterminer si cette décision doit être liée à une autre procédure (p. ex. procédure fiscale) ou si elle doit être prise de manière indépendante. Signalons enfin qu'un refus ou une restriction du droit d'accès doit également revêtir la forme d'une décision.

Le 5^e alinéa prévoit une *voie de droit* spéciale pour les causes relevant du droit de la protection des données. Les décisions en la matière ne peuvent être portées devant l'autorité de surveillance, elles doivent l'être devant la Commission fédérale de la protection des données (cf. art. 27).

221.5 Section 5: Le préposé fédéral à la protection des données

Article 23 Nomination et statut

A elles seules, des normes de comportement ne permettent pas d'obtenir une protection des données efficace. Si l'on entend assurer le respect des principes de protection des données que renferme le projet, il est impératif d'instituer un organe de surveillance et surtout de conseil. La procédure de consultation n'a pas remis fondamentalement en question la nécessité d'un contrôle; et ce, même si quelques divergences quant aux modalités de celui-ci sont apparues. Le présent projet institue une instance de surveillance en matière de protection des données aussi efficace que simple et proche de l'administré. Dès lors il confie la surveillance en grande partie à un *préposé à la protection des données*, et non, comme le prévoyait l'avant-projet, à une institution relativement lourde et complexe, à savoir à une commission de la protection des données composée de treize membres. Cela dit, les litiges en matière de protection des données seront du ressort d'une *Commission de la protection des données* qui fonctionnera comme instance de recours et d'arbitrage au sens du projet de révision de la loi fédérale sur l'organisation judiciaire. Si les compétences du préposé et de la commission sont particulièrement étendues dans le secteur public, elles sont en revanche beaucoup plus restreintes dans le secteur privé, puisqu'elles se limitent aux traitements à hauts risques.

Suivant le 1^{er} alinéa la nomination du préposé est du ressort du Conseil fédéral. Il appartiendra en outre à celui-ci de préciser les conditions d'engagement soit de manière générale dans une ordonnance, soit de manière spécifique dans les cas d'espèce. On relèvera qu'en règle générale, le préposé sera soumis au statut des fonctionnaires et, dans tous les cas, au secret de fonction.

A la teneur du 2^e alinéa le préposé s'acquittera de ses tâches de manière autonome. Il sera rattaché administrativement au Département fédéral de justice et police. Si le préposé est rattaché au Département fédéral de justice et police, c'est parce qu'il devra traiter avant tout des questions juridiques, à l'instar de ce département.

Le 3^e alinéa prévoit que le préposé disposera de son propre secrétariat; il appartiendra au Conseil fédéral d'en prévoir le financement dans le cadre du budget.

Article 24 Surveillance

Cette disposition définit les compétences du préposé à la protection des données. Il a principalement le pouvoir d'ouvrir une *enquête* lorsqu'il soupçonne une éventuelle atteinte à la personnalité, et d'adresser des *recommandations* à ceux qui traitent les données. Il peut aussi informer de ses constatations les personnes concernées. Il lui est en revanche impossible de prendre des mesures contraignantes.

Suivant le 1^{er} *alinéa* le préposé ne doit pas seulement veiller au respect de la seule loi, mais également de tous les textes légaux fédéraux qui contiennent des dispositions de protection des données, c'est-à-dire non seulement la législation spéciale sur la protection des données, en vigueur ou future, mais également les traités internationaux. Il est en outre précisé que le Conseil fédéral échappe à la surveillance du préposé; ce dernier ne peut pas, en effet, surveiller ceux qui sont appelés à le surveiller. Cela ne signifie pas pour autant que le Conseil fédéral soit dispensé de se conformer aux dispositions sur la protection des données.

Selon le 2^e *alinéa* le préposé peut ouvrir une enquête d'office ou sur plainte pour autant qu'il juge nécessaire d'élucider les faits. Reste que le préposé ne sera pas en mesure de se pencher sur tous les traitements qui s'avèreraient discutables du point de vue de la protection des données; il devra dès lors se contenter des cas les plus importants ou de ceux qui pourront avoir une valeur de précédent. Ainsi, celui qui porte plainte contre la violation réelle ou présumée d'une disposition de protection des données ne doit pas nécessairement s'attendre à un résultat; il n'y a pas un droit. En outre, le préposé ne pourra qu'exceptionnellement ouvrir une enquête à l'encontre de traitements effectués par des privés. Conformément au principe de l'autonomie privée, qui prévaut en droit civil, les atteintes à la personnalité causées par des traitements effectués par des personnes privées sont l'affaire de la personne concernée et non d'une autorité étatique. Il s'ensuit que les prétentions qui en découlent doivent être portées devant le juge civil. Le projet prévoit cependant trois exceptions à ce principe: le préposé peut intervenir dans le secteur privé si une personne privée recourt à une méthode de traitement susceptible de porter atteinte à la personnalité d'un nombre important de personnes (let. a). Cette disposition vise les *défauts inhérents à la conception même du système*, défauts auxquels il ne peut être convenablement remédié par les voies de la procédure civile. Il importe dès lors que le préposé dispose, pour des raisons quasiment d'intérêt public, de pouvoirs d'enquête. Etant donné les hauts risques d'atteinte à la personnalité liés à l'exploitation de fichiers soumis à l'*obligation d'enregistrement* et à la *communication de données à l'étranger soumise à déclaration*, il importe, dans ces deux cas également, d'habiliter le préposé à élucider les faits (let. b et c). Le préposé doit être à même de prendre les mesures qui s'imposent à chaque fois qu'il constate qu'un traitement de données menace la personnalité; à défaut, les obligations d'enregistrer et d'annoncer seraient sans portée pratique. Du moment qu'une obligation très limitée d'enregistrer les fichiers incombe à ceux qui traitent des données à titre privé, le préposé ne bénéficiera que de compétences très restreintes dans ce domaine. Lorsque des données sont traitées par les organes fédéraux, en revanche, le préposé est en droit de procéder à toute investigation qu'il juge nécessaire (let. d). Un contrôle

aussi étendu s'explique par le fait que l'administration est soumise sans restriction aucune au principe de légalité.

Le 3^e alinéa octroie au préposé la *compétence de requérir toutes les informations* nécessaires à la conduite de ses enquêtes. Il a ainsi le droit d'exiger la production de pièces; à cet égard, les documents relatifs à la conception des systèmes informatiques devraient retenir toute son attention. Si le délégué entend juger de l'impact réel des traitements, il pourra toujours se les faire présenter sur place. Le préposé doit en outre être en droit d'obtenir des informations non seulement de ceux qui ont la responsabilité des traitements ou des maîtres de fichiers, mais également de leurs auxiliaires. On relèvera que toute personne impliquée dans l'enquête est tenue de collaborer à l'établissement des faits; cette collaboration est en tous points semblable à celle qui est prévue à l'article 13 de la loi fédérale sur la procédure administrative (RS 172.021). Si les personnes privées et les organes fédéraux sont tenus de collaborer, elles sont toutefois dispensées de donner des informations qui pourraient en définitive leur porter préjudice. C'est pourquoi le 3^e alinéa prévoit qu'une personne impliquée dans une enquête conduite par le préposé peut refuser de témoigner; l'article 16 de la loi sur la procédure administrative fédérale, et, en partie, l'article 42, 1^{er} et 2^e alinéas, de la loi fédérale de procédure civile fédérale (RS 273) sont applicables par analogie. C'est ainsi que celui qui traite les données, voire une tierce personne, peut refuser de donner toute information qui exposerait lui-même ou des proches à des poursuites pénales, notamment pour violation des articles 28 et 29 du présent projet. Les personnes appelées à témoigner peuvent aussi opposer au préposé le secret professionnel. Toutefois, la personne concernée peut les en délier. Le secret de fonction ne peut pas, par contre, être opposé au préposé.

Si le préposé à la protection des données, à la suite de l'enquête qu'il a menée, parvient à la conclusion qu'un traitement a violé les prescriptions de la loi, il adresse une *recommandation* selon le 4^e alinéa. Par elle, il invitera en règle générale celui qui traite des données à modifier sa pratique. Il n'a pas besoin pour cela de se référer à un cas d'espèce. Il est toutefois envisageable que le préposé axe sa recommandation sur une personne déterminée ou sur un groupe de personnes. L'injonction n'a cependant aucun caractère contraignant, ni pour ceux qui traitent les données à titre privé, ni pour les organes fédéraux. Il ne s'agit donc *nullement d'une décision* qui peut être mise en œuvre par le biais de l'exécution forcée. Il s'ensuit que les personnes privées et les organes fédéraux sont libres de se conformer à la recommandation ou non. Toutefois, s'ils optent pour le second terme de l'alternative, ils risquent de voir le traitement litigieux déclaré illicite à la suite d'une action fondée sur le droit privé ou d'un recours administratif, ce qui peut avoir pour conséquence, le cas échéant, d'engager leur responsabilité civile ou pénale. En outre, ils doivent s'attendre à ce que le préposé porte l'affaire devant la commission de la protection des données; celle-ci peut alors constater le caractère illicite du traitement dans une *décision contraignante*.

Le préposé invite le destinataire d'une recommandation à déclarer, en temps utile, s'il entend s'y conformer ou non. Si le préposé ne reçoit aucune réponse ou reçoit une réponse négative, ou encore s'il constate que le traitement litigieux est poursuivi en dépit d'une déclaration d'acceptation de la recommandation, il peut, s'il le juge opportun, porter l'affaire devant la Commission fédérale de la

protection des données en vertu du 5^e *alinéa*, lettre a. Le préposé sera tout particulièrement enclin à saisir la commission si d'importants intérêts publics sont en jeu ou s'il s'agit de questions pouvant avoir valeur de précédent. Par contre, si aucun intérêt public n'étant en jeu, seules quelques personnes sont touchées par le traitement illicite, le préposé pourra renoncer à saisir la commission et se limiter à indiquer à la personne concernée qui s'est adressée à lui les voies de droit possibles (let. b). C'est alors à elle qu'il appartient d'introduire, le cas échéant, une action fondée sur l'article 12 ou d'émettre une prétention sur la base de l'article 22. Lorsque la Commission de la protection des données est saisie, elle rend une décision après réexamen de la question. Relevons enfin qu'en règle générale la personne concernée sera rarement associée à la procédure: les recommandations du préposé seront en effet d'une portée très générale.

Article 25 Informations

Les exemples étrangers le montrent à suffisance: la protection des données ne peut s'imposer que si les organes qui en sont chargés ont la possibilité d'informer sur leurs activités et de donner à celles-ci une certaine publicité. Suivant le 1^{er} *alinéa* le préposé doit faire rapport au Conseil fédéral, à intervalles réguliers et selon les besoins. Les rapports périodiques sont des rapports d'activités qui seront publiés. Quant aux autres rapports, le Conseil fédéral décidera, en l'espèce, de leur publication.

En vertu du 2^e *alinéa*, le préposé a encore la possibilité, s'il en va de l'intérêt général, de s'adresser directement au public. Tel sera certainement le cas pour une recommandation concernant un système informatique d'importance nationale. Il ne peut toutefois porter à la connaissance du public des données soumises au secret de fonction qu'avec le consentement de l'autorité compétente. Cela dit, il importe que cette dernière ne puisse pas tirer parti de cet *alinéa* pour empêcher la révélation de manquements; à cet effet, il est prévu que les différends entre le préposé et l'autorité compétente peuvent être portés devant le président de la Commission de la protection des données. Sa décision est définitive.

Article 26 Autres attributions

Si la surveillance est assurément la tâche primordiale du préposé, ce n'est pas la seule: le 1^{er} *alinéa* définit ses autres attributions. Etant donné qu'il disposera de vastes connaissances et, surtout d'une expérience pratique unique, le préposé sera particulièrement à même de conseiller les personnes privées, de même que les organes fédéraux et cantonaux, en matière de protection des données; il est ainsi également tout destiné à prévenir les conflits en matière de protection des données en fonctionnant comme médiateur (let. a). Au surplus, il lui appartiendra de se prononcer sur les projets d'actes législatifs fédéraux qui revêtiront de l'importance pour la protection des données (let. b). Le préposé devra en outre collaborer avec les autorités chargées de la protection des données en Suisse et à l'étranger (let. c). A cet égard, il se devra de promouvoir les échanges d'informations entre les organes chargés de la protection des données au niveau de la Confédération et des cantons. Ces tâches ne sont pas nouvelles: elles sont aujourd'hui déjà remplies par le service de la protection des données de l'Office fédéral de la justice. D'un autre côté, le préposé aura soin d'assurer l'entraide

administrative prévue par les articles 13 et suivants de la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Il informera les autorités étrangères, à leur demande, sur le droit et la pratique administrative suisse en matière de protection des données; de même, il leur fournira des renseignements concrets sur les traitements automatisés de données effectués dans notre pays. Enfin, il sera parfaitement à même d'apprécier dans quelle mesure la protection des données assurée à l'étranger est comparable à celle que connaît la Suisse. Ainsi, le cas échéant, il lui appartiendra de fournir aux personnes privées comme aux autorités des avis sur la mesure dans laquelle un transfert de données à l'étranger au sens de l'article 4, 5^e alinéa, viendrait à menacer sérieusement la personnalité des personnes concernées (let. d).

Les domaines dans lesquels la présente loi s'applique ne sont pas les seuls à connaître des problèmes de protection des données. Dès lors, il importe que les organes fédéraux puissent, aux termes de 2^e alinéa également, demander au préposé des conseils dans d'autres domaines. De son côté, le préposé peut solliciter la présentation de traitements des autorités qui ne sont pas soumises à la loi sur la protection des données en vertu de l'article 2, tels les services chargés de tenir les registres publics, de conduire des recherches policières préliminaires, d'assurer l'entraide judiciaire internationale et de conduire les procédures pénales administratives, ainsi que les instances de recours administratif. Afin que le préposé puisse se faire une image précise des problèmes éventuels, il est nécessaire que ces autorités puissent lui accorder l'accès à leurs dossiers. A cet égard, le 2^e alinéa doit être considéré comme une exception au principe du secret de fonction posé par l'article 27 du statut des fonctionnaires et à l'obligation de témoigner instituée par l'article 28 de ce même statut.

Le 3^e alinéa règle les attributions du préposé à la protection des données lorsqu'il collabore avec la Commission du secret professionnel en matière de recherche médicale (cf. ch. 222.43).

221.6 Section 6: Commission fédérale de la protection des données

Article 27

En créant une *Commission fédérale de la protection des données*, la loi entend consacrer la protection juridique la plus large possible dans le secteur public. Aux termes du 1^{er} alinéa cette commission n'est rien d'autre qu'une commission d'arbitrage et de recours au sens des dispositions sur la procédure administrative contenues dans le projet de révision de la loi fédérale sur l'organisation judiciaire⁵¹). Le droit de la protection des données respecte ainsi la philosophie de cette révision: d'une part le nombre des instances de recours administratif est réduit, d'autre part la création d'une autorité judiciaire administrative spécialisée décharge le Tribunal fédéral. Les nouvelles dispositions sur la procédure de recours administratif s'appliqueront donc à la Commission fédérale de la protection des données. Elle sera composée de sept membres; le Conseil fédéral pourra prévoir par voie réglementaire que la commission se divise en deux sections, l'une

+ exercera ses compétences pour le secteur public, l'autre pour le secteur privé. Conformément aux règles générales applicables aux commissions de recours et d'arbitrage, la Commission de la protection des données siégera à cinq membres lorsqu'elle est saisie d'une question juridique d'importance fondamentale, à trois membres pour les autres affaires.

Le 2^e alinéa définit les attributions de la commission. Celle-ci statue en première instance sur les recommandations que le préposé a faites à la suite d'une enquête (art. 24) et qu'il a soumises à la commission pour décision. En outre, la commission se prononce en deuxième instance sur les recours contre les décisions des organes fédéraux en matière de protection des données (let. b), telle une décision concernant le droit d'accès ou une requête en rectification ou en destruction des données au sens de l'article 22. Sont toutefois exceptées les décisions du Conseil fédéral. Par ailleurs, en deuxième instance, la commission tranche aussi les recours contre les décisions de la commission du secret professionnel en matière de recherche médicale (let. c; cf. nos remarques ch. 222.43). Enfin, les décisions cantonales de dernière instance prises en application des dispositions du droit public fédéral relatives à la protection des données peuvent être portées devant la commission (let. d). Certes, la présente loi ne régit pas les traitements de données effectués par des organes cantonaux; cependant, certaines dispositions fédérales spéciales de protection des données – notamment en droit des étrangers et en droit des assurances sociales – leur sont applicables.

La réglementation prévue aux lettres b et d a pour conséquence que l'instance qui statuera sur les prétentions de protection des données fondées uniquement sur la présente loi n'est pas l'autorité de recours habituellement compétente du fait de la matière. Cette diversification des voies de droit est justifiée par la nécessité de créer, dès le début de l'application de la loi, une unité de jurisprudence. Toutefois, du moment que les décisions de la commission peuvent être portées, par la voie du recours de droit administratif, devant le Tribunal fédéral, il est dès lors garanti que ce dernier examinera l'application de la loi indépendamment du contexte. Relevons qu'il peut arriver qu'une personne fasse valoir, en même temps qu'une prétention fondée sur la loi, d'autres prétentions qui n'ont rien à voir avec la protection des données. Tel serait le cas d'une demande en rectification des données auprès de l'assurance invalidité qui permettrait de fonder une demande de rente d'invalidité plus élevée. La prétention principale ne relevant pas de la protection des données proprement dite, une telle demande devrait suivre la procédure ordinaire. La commission n'a pas, en effet, à entrer en matière sur des questions de protection des données qui ne sont en fait que des questions préjudicielles tendant à fonder d'autres demandes.

Il est très possible que le préposé, à l'occasion d'une enquête, vienne à découvrir un traitement qui doit être aussitôt modifié ou abandonné sous peine de causer de graves dommages à une personne. Dans ce cas, le 3^e alinéa permettra au préposé de demander au président de la Commission de la protection des données de prendre des *mesures provisionnelles*. La personne concernée a la possibilité de faire de même: elle se fondera sur l'article 28c du code civil s'agissant du secteur privé, sur l'article 56 de la loi sur la procédure administrative s'agissant du secteur public.

221.7 Section 7: Dispositions pénales

En principe, il n'y a pas lieu de réprimer les violations des dispositions de la loi sur la protection des données au moyen de sanctions pénales, mais au moyen de sanctions civiles ou administratives. Le projet prévoit cependant trois exceptions à cette règle. D'abord, l'article 28 sanctionne pénalement la personne privée qui viole l'obligation de renseigner, ou celle d'annoncer, ou encore celle de collaborer; en effet, de ces obligations dépend en grande partie l'efficacité même de la loi sur la protection des données, car elles assurent *une certaine transparence* des traitements effectués. Est également sanctionnable pénalement, celui qui révèle des données personnelles secrètes et sensibles dont il a eu connaissance dans l'exercice de sa profession (art. 29). En faisant appel à un spécialiste et en lui confiant des données, la personne concernée crée une relation de confiance qui doit être à tout prix réservée. Enfin, il importe que la soustraction de données personnelles soit punissable (art. 179^{novies} CP). Les deux premières infractions mentionnées ne sont que de simples contraventions qui ont leur place dans la loi sur la protection des données; la troisième infraction en revanche est un délit en affinité certaine avec le titre troisième du code pénal: infractions contre l'honneur et contre le domaine secret ou le domaine privé; sa place est dans le code pénal. La poursuite de ces infractions est l'affaire des cantons.

Article 28 Violation des obligations de renseigner, d'annoncer et de collaborer
Suivant le *1^{er} alinéa*, est passible des arrêts ou de l'amende, la personne privée, maître du fichier, qui viole l'obligation de renseigner instituée à l'article 5 ou qui refuse de fournir les renseignements sans indiquer les motifs au sens de l'article 6, *2^e alinéa*. Se rend coupable de cette infraction non seulement le maître du fichier qui fournit un renseignement inexact, mais aussi celui qui donne des informations incomplètes tout en laissant croire que celles-ci sont complètes. N'est en revanche pas punissable celui qui, invoquant l'article 6, prétend qu'il n'est pas tenu à fournir de renseignements. Dans ce cas, seule une action de droit civil permet de savoir si le refus ou la restriction du droit d'accès est justifiée ou non. En revanche, la personne qui, contre la vérité, prétend ne détenir aucune information sur la personne concernée tombe sous le coup de l'article 28, *1^{er} alinéa*. Agit *intentionnellement* au sens de la disposition, celui qui connaît le caractère inexact ou incomplet des renseignements qu'il donne. Commet un *dol éventuel*, le maître du fichier qui fournit un renseignement, sans aucune vérification, alors même qu'il doute du caractère exact de celui-ci. La violation de l'obligation de renseigner est une infraction qui se punit sur plainte.

Le *2^e alinéa* sanctionne les personnes privées qui n'auront pas rempli leur obligation de déclarer un fichier ou un transfert de données à l'étranger ou encore auront fourni, à cette occasion, des indications inexactes ou incomplètes (let. a); cette infraction est punissable d'office. Est punissable celui qui a agi intentionnellement, autrement dit celui qui entendait volontairement se soustraire à l'une ou l'autre desdites obligations. Celui qui simplement n'en avait pas connaissance, peut se prévaloir de l'erreur de droit; dans ce cas, le juge pourra soit l'exempter de toute peine, soit en réduire la quotité⁵²). Enfin, sont également punissables les personnes privées qui auront fourni des renseignements inexactes

lors d'une enquête conduite par le préposé ou lui auront refusé sa collaboration (let. b). Le préposé devrait ainsi être en mesure d'obtenir toutes les informations qui lui sont nécessaires.

Nous avons renoncé à soumettre les organes fédéraux à ces dispositions car il existe déjà dans l'administration une surveillance des services et les fonctionnaires qui faillissent à leur devoir, contrairement aux personnes privées, peuvent être amenés à rendre des comptes par le biais de mesures disciplinaires. Par ailleurs, la surveillance du préposé à la protection des données dans le secteur public est plus étendue. Relevons en outre qu'il serait pour le moins inhabituel de permettre à une autorité fédérale, tel le préposé à la protection des données, de déposer plainte pénale contre un fonctionnaire ou un office, pour le motif qu'elle s'est vue refuser des informations à titre d'entraide administrative. Dans de tels cas, en effet, il appartient à l'autorité hiérarchiquement supérieure et, en dernière instance, au Conseil fédéral de se prononcer sur l'entraide.

Article 29 Violation du devoir de discrétion

Du fait que les activités professionnelles se spécialisent toujours plus, du fait également que les méthodes de traitement de l'information sont toujours plus sophistiquées, la protection du secret professionnel instituée par l'article 321 du code pénal est devenue insuffisante. Cette norme ne régit que les ecclésiastiques, les avocats, les défenseurs en justice, les notaires, les contrôleurs astreints au secret professionnel en vertu du code des obligations, les médecins, les dentistes, les pharmaciens, les sages-femmes ainsi que leurs auxiliaires. La nouvelle disposition entend donc soumettre au devoir de discrétion qui s'impose certaines activités professionnelles qui ne sont pas régies par l'article 321 du code pénal. Il aurait été possible d'étendre le champ d'application de l'article 321 du code pénal à d'autres catégories professionnelles; cette solution n'a pas été retenue, car les professions mentionnées à l'article 321 bénéficient en général du droit de refuser de témoigner prévu par les lois de procédure fédérales et cantonales; un droit qu'il n'aurait pas été opportun d'étendre par le biais de la législation sur la protection des données. La nécessité ou non de réviser l'article 321 sera toutefois examinée lors de la révision de la partie générale du code pénal.

Seul se rendra coupable de l'infraction instituée par le *1^{er} alinéa* celui qui exerce une profession qui requiert la connaissance de données personnelles secrètes et sensibles. Tel est le cas des psychologues, des assistants sociaux ou des conseillers conjugaux; les coiffeurs en revanche n'entrent pas dans cette catégorie. Il est vrai que ceux-ci peuvent avoir connaissance, dans l'exercice de leur profession, de données personnelles secrètes et sensibles; celles-ci ne leur sont toutefois pas nécessaires pour exercer leur profession. La présente norme pénale doit être considérée comme un *délit de fonction proprement dit*; en effet, elle n'est pas applicable à tout-un-chacun, mais seulement à certaines catégories professionnelles. L'élément constitutif de l'infraction est la *donnée personnelle secrète* ayant un caractère *sensible* au sens de l'article 3, lettre e. Se prononçant sur les articles 162 (violation du secret de fabrication ou du secret commercial) et 321 (violation du secret professionnel) du code pénal, la doctrine et la jurisprudence sont d'avis que toute donnée qui est dans une certaine mesure inconnue doit être considérée comme secrète; autrement dit, il s'agit de données ni notoires ni accessibles à tout

le monde que la personne concernée entend, à juste titre, garder secrètes. L'infraction n'est punissable que si elle a été commise intentionnellement. Celui qui ignore qu'il est tenu de garder le secret peut invoquer l'erreur de droit au sens de l'article 20 du code pénal. La peine est les arrêts ou l'amende. On relèvera enfin que la contravention instituée par l'article 29 du présent projet ne se poursuit que sur plainte.

Le 2^e *alinéa* rend également punissables les auxiliaires de la personne soumise, en vertu du 1^{er} *alinéa* à l'obligation de garder le secret qui révèlent intentionnellement des données personnelles secrètes et sensibles. Concrètement, la disposition vise les employés et les apprentis.

Suivant le 3^e *alinéa* la protection pénale ne s'éteint pas avec la cessation de l'activité, des rapports de travail ou de la formation.

221.8 Section 8: Dispositions finales

Article 30 Exécution

Le 1^{er} *alinéa* rappelle la compétence réglementaire générale du Conseil fédéral déjà mentionnée dans la constitution.

Les *alinéas* suivants octroient au Conseil fédéral des compétences qui ne sauraient découler directement de son pouvoir réglementaire. Ainsi aux termes du 2^e *alinéa* le Conseil fédéral édicte des dispositions spécifiques régissant le traitement des données personnelles déposées aux Archives fédérales. Il peut prévoir des dérogations aux règles sur le droit d'accès (art. 5 et 6) et sur le traitement de données sensibles (art. 14, 2^e al., et 16, 1^{er} al.). De telles dérogations peuvent se justifier car l'archivage de documents permet déjà de restreindre l'accès. Il est vrai que la masse de données déposée aux Archives fédérales peut encore être en règle générale consultée d'après les personnes; toutefois, une telle consultation requiert la mise en œuvre de moyens importants. Parmi les données archivées, on trouve nombre de données sensibles; cependant, une fois le délai de non-consultation écoulé, leur traitement ne doit pas nécessairement reposer sur une base légale expresse dans une loi au sens formel ou sur une autorisation préalable du Conseil fédéral.

Conformément au 3^e *alinéa*, le Conseil fédéral peut aussi déroger aux règles sur le droit d'accès en faveur des représentations diplomatiques et consulaires de la Suisse à l'étranger. En effet, il pourrait se révéler délicat pour les représentations de devoir donner des renseignements sur un étranger à l'étranger car cela pourrait compromettre les relations avec l'Etat dont la personne concernée est le ressortissant.

Le 4^e *alinéa* attribue au Conseil fédéral trois autres compétences spéciales. Ainsi, il devra déterminer les fichiers dont le traitement doit faire l'objet d'un *règlement* (let. a). Il importe en effet que pour chacun des grands fichiers à fins multiples, en particulier pour ceux qui dépendent de systèmes dits «répartis», les principes de la présente loi soient spécifiquement concrétisés. Ces règlements de traitement assurent en outre une certaine transparence des processus de traitement, et partant en facilitent le contrôle. Le Conseil fédéral pourra se fonder sur l'actuel

†
registre des fichiers de l'administration fédérale pour déterminer quels fichiers devront faire l'objet d'un règlement. En outre, il appartiendra au Conseil fédéral de spécifier sous quelle condition *un tiers* – notamment une personne privée – *peut traiter des données pour le compte d'un organe fédéral* d'une part, un organe fédéral peut effectuer un traitement pour le compte d'un autre service administratif ou d'une personne privée d'autre part (let. b). Cela dit, le Conseil fédéral devra apprécier dans quelle mesure un traitement effectué en relation avec l'accomplissement d'une tâche publique peut être confié à une personne privée et si de ce fait, il peut en résulter des problèmes spécifiques de sécurité des données. Enfin, il devra encore déterminer selon quel mode les moyens d'identification de personnes peuvent être utilisés (let. c). Parallèlement au développement toujours plus rapide du traitement automatisé des données, les mesures de sécurité des données sont devenues toujours plus sophistiquées; cela vaut tout particulièrement pour les contrôles d'accès aux systèmes informatisés. A cet égard, l'identification joue un rôle central. Les techniques d'identification des personnes se multiplient: jusqu'à peu, on avait surtout recours à des mots de passe, à des badges ou aux empreintes digitales; aujourd'hui, on peut identifier une personne sur la base des caractéristiques de sa rétine ou de ses cheveux. Il importe que le Conseil fédéral soit en droit de réglementer le recours à ces moyens d'identification, car ils constituent tous une atteinte à la personnalité. En outre, il importe de limiter l'usage des moyens d'identification traditionnels, tel le numéro AVS. L'usage de cette identification est aujourd'hui tellement répandu que l'interconnexion des nombreuses informations qui en dépendent permettrait d'obtenir un profil complet de la personnalité.

Le 5^e *alinéa* octroie au Conseil fédéral la compétence de conclure des traités internationaux en matière de protection des données. Reste que la conclusion de traités qui dérogent à la loi demeure de la compétence de l'Assemblée fédérale.

Suivant le 6^e *alinéa* le Conseil fédéral peut réglementer la manière de protéger et de mettre en sûreté les fichiers et ce, au titre de mesures s'inscrivant dans le cadre de la défense générale. Certains fichiers, à commencer par les listes des membres de partis politiques ne peuvent tomber aux mains d'un éventuel agresseur sans faire courir de sérieux dangers aux personnes concernées.

Article 31 Dispositions transitoires

Suivant le 1^{er} *alinéa* les organes fédéraux, comme les personnes qui traitent des données à titre privé, doivent déclarer au préposé dans le délai d'une année à compter de l'entrée en vigueur de la loi les fichiers existants qui doivent être annoncés.

Ils doivent également, aux termes du 2^e *alinéa* prendre, dans le délai imparti, toutes les mesures nécessaires à assurer l'exercice du droit d'accès au sens de l'article 5. De fait, les maîtres des fichiers disposent d'un délai légèrement plus long pour se conformer à ces prescriptions; il faut en effet tenir compte du laps de temps séparant l'adoption de la loi de son entrée en vigueur.

Aux termes du 3^e *alinéa* les organes fédéraux peuvent continuer à utiliser pendant cinq ans les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité, quand bien même les sévères conditions de traitement posées

par l'article 14, deuxième alinéa, ne sont pas réunies. Il est en effet matériellement impossible de créer d'un jour à l'autre les bases légales exigées par cette disposition.

222 Annexe: Modification de lois fédérales

222.1 Protection des données dans les relations de travail

Articles 328b (nouveau) et 362 CO

Si nous proposons d'introduire un *article 328b* dans le code des obligations, c'est parce qu'il importe de protéger la personnalité du *travailleur* au moyen d'une disposition de protection des données spécifique. Dans la foulée, il est nécessaire d'étendre la portée de l'*article 362* du code des obligations en complétant la liste des dispositions du code auxquelles il ne peut être dérogé au détriment du travailleur. Ces compléments apportés à la législation sur le contrat de travail sont indispensables; en effet, plus qu'aucun autre rapport juridique, le rapport de travail donne lieu à la collecte et au traitement de données personnelles de toute nature et pendant une longue durée. Il se justifie également d'accorder une protection particulière au travailleur, car il dépend en fait et en droit de son employeur. L'*article 328b (nouveau)* du code des obligations complète la loi sur la protection des données en ce sens qu'il détermine la nature des informations que l'employeur est en droit de traiter sur ses employés, qu'il spécifie dans quels cas celui-là peut donner à des tiers des renseignements à leur sujet, enfin, qu'il accorde aux employés un droit d'accès.

Selon le *1^{er} alinéa* de l'*article 328b*, seuls sont licites les traitements de données personnelles qui portent sur les aptitudes du travailleur à remplir son emploi ou qui sont nécessaires à l'exécution du contrat de travail. Le *1^{er} alinéa* concrétise ainsi le principe général de la proportionnalité posé à l'article 4, 3^e alinéa, de la loi sur la protection des données. Certes, l'objectivité des décisions relatives au personnel, de même que la protection de la personnalité des employés ont tout à gagner de la rationalisation de la gestion du personnel au moyen des méthodes modernes de traitement des données; ces méthodes sophistiquées n'ont cependant pas que des effets positifs: elles sont de nature à révéler presque toutes les facettes de la personnalité d'un employé, transparence que ne justifient en aucun cas les besoins réels de l'entreprise.

Le *2^e alinéa* de l'*article 328b* dispose que l'employeur ne peut donner à des tiers des renseignements sur le travailleur que si une disposition légale l'y autorise ou si le travailleur y a consenti. A ce jour, la législation sur le droit du travail ne connaît aucune disposition imposant expressément à l'employeur une obligation de garder le secret. La réglementation sur le certificat de travail fait cependant, dans une certaine mesure, exception: le travailleur qui s'attend à recevoir un certificat qui pourrait lui être préjudiciable peut demander une simple attestation de travail (art. 330, let a, 2^e al., CO)⁵³. Reste qu'en pratique un employeur cherche à s'informer sur un candidat à un emploi auprès de ses anciens employeurs; ce qui revient à tourner la réglementation sur l'attestation de travail. Partant, on fait peu de cas du droit du travailleur à l'autodétermination sur ses données personnelles. Il importe dès lors d'instituer une réglementation idoine dans la législation sur le contrat de travail.

Le 3^e alinéa accorde au travailleur le droit de *consulter* son dossier personnel et renvoie, en ce qui concerne les modalités de l'exercice de ce droit, aux règles sur le droit d'accès contenues dans la loi sur la protection des données. Pour l'employeur, il est dans bien des cas beaucoup plus simple de laisser le travailleur consulter son dossier personnel plutôt que de lui donner un renseignement; ce procédé a en outre l'avantage de garantir un accès intégral aux informations. L'employeur qui se soustrait à l'obligation qui lui est faite de donner accès au dossier, notamment parce qu'il tient un dossier noir, est punissable en vertu de l'article 28, 1^{er} alinéa, de la loi sur la protection des données. Cela dit, l'employeur peut toutefois se prévaloir de l'un ou l'autre des motifs énoncés à l'article 6 pour restreindre l'accès.

222.2 Droit international privé: compétence et droit applicable dans les litiges de protection des données

Article 130, 3^e alinéa, et 139, 3^e alinéa, LDIP

Les règles de conflit prévues par la loi fédérale sur le droit international privé (LDIP) sont insuffisantes pour régler tous les problèmes de compétence et de choix de droit qui peuvent se présenter à l'occasion des litiges de droit international privé en matière de protection des données. La loi sur le droit international privé⁵⁴⁾ doit être ainsi complétée par deux dispositions de protection des données: la première concerne la *compétence des tribunaux suisses* à se prononcer sur les actions en exécution du droit d'accès; la seconde, le *droit applicable*.

Suivant l'article 130, 3^e alinéa, les actions en exécution du droit d'accès dirigées contre le maître du fichier peuvent être intentées devant les tribunaux suisses de son domicile ou, le cas échéant, devant les tribunaux de son lieu de séjour ou d'établissement. On ne peut cependant obliger la personne concernée à actionner le maître du fichier devant un juge étranger du simple fait que le maître du fichier séjourne à l'étranger. Dès lors, il se justifie de permettre à la personne concernée d'intenter son action devant le juge du lieu où le fichier est géré ou utilisé.

L'article 139, 3^e alinéa, LDIP, accorde à la personne concernée le choix du droit applicable. Elle peut faire valoir les prétentions découlant d'une atteinte à la personnalité du fait d'un traitement de données personnelles ou les prétentions découlant d'entraves mises à l'exercice du droit d'accès soit d'après le droit de l'Etat de sa résidence habituelle, soit d'après le droit de l'Etat où s'est produit le résultat de l'atteinte ou de l'entrave, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans ces Etats. La personne concernée peut aussi faire valoir ses prétentions d'après le droit de l'Etat dans lequel l'auteur de l'atteinte ou de l'entrave a son établissement ou sa résidence habituelle. Celui qui traite des données n'a ainsi plus la possibilité de porter préjudice à la personne concernée en se choisissant un domicile avantageux au regard de la protection des données. D'un autre côté, la liberté du choix de droit ne permet pas à celui qui traite les données de spéculer sur le régime juridique applicable. Il s'agit là d'un problème qui n'est pas spécifique au droit de la protection des données; du fait de l'internationalisation croissante de l'économie, ce problème touche aussi d'autres domaines.

222.3 Soustraction de données personnelles

Article 179^{novies} (nouveau) CP

En substance, cette disposition se rapproche de l'article 143 du code pénal (CP) dans sa nouvelle teneur proposée par la commission d'experts chargée de réviser les dispositions du code pénal concernant les délits contre le patrimoine; cette disposition a été mise en consultation en 1985 et en 1986. Le projet d'article 143 protège avant tout le patrimoine de celui qui traite des données et non la personnalité de la personne concernée. De ce fait, des voix se sont élevées lors de ladite procédure de consultation pour exiger que la collecte de données personnelles soit réglementée de manière générale, notamment sous l'angle de la protection de la personnalité. Il y a dès lors lieu de tirer parti de la création de la loi sur la protection des données pour compléter les dispositions du code pénal sanctionnant les infractions contre le domaine secret ou le domaine privé (art. 179 ss) par une nouvelle norme sanctionnant la soustraction de données personnelles sensibles.

Les données personnelles sensibles qui ne sont pas librement accessibles sont l'élément constitutif du délit institué à l'article 179^{novies}. Ces données sont définies à l'article 3, lettre e. Autrement dit, est punissable celui qui a eu connaissance de ces données en s'introduisant dans des locaux ou des installations dont l'accès lui était interdit. L'auteur de l'infraction peut parvenir à prendre connaissance des données de différentes manières: il peut dérober des dossiers entiers ou partie de ceux-ci, il peut s'introduire dans le système à partir d'un terminal, ou encore il peut intercepter des transmissions de données. Reste que l'auteur de l'infraction n'est punissable que s'il a agi intentionnellement. Le délit institué par l'article 179^{novies} n'est poursuivi que sur plainte. Celle-ci peut être déposée tant par la personne concernée que par celui qui traite les données. Relevons enfin que la soustraction illicite de données est un délit passible de l'emprisonnement ou de l'amende.

222.4 Protection des données dans la recherche médicale

222.41 Les impératifs d'ordre constitutionnel

La recherche médicale se pratique avant tout dans les universités et les hôpitaux (publics ou privés); celle effectuée par la Confédération n'a à cet égard qu'une importance mineure. Le droit constitutionnel ne permet pas de régler le traitement de données dans ces différents domaines de manière satisfaisante. Si la Confédération peut se fonder sur les articles 64 et 85, chiffre 1, cst., pour réglementer la protection des données dans le cadre de ses propres recherches ou de celles effectuées par des privés, elle est en revanche dépourvue de toute compétence pour légiférer dans le domaine du droit public cantonal, droit qui régit les universités et les hôpitaux cantonaux, régionaux et communaux. Il appartient à la législation cantonale sur la protection des données – si une telle législation a été instituée – de régir ces cas. L'article 27^{sexies} cst. relatif à la recherche n'y change rien. S'il donne à la Confédération la compétence d'encourager la recherche scientifique, il maintient en revanche la répartition des

compétences dans les domaines de la formation universitaire et de la recherche. Ainsi, la formation universitaire – exception faite des écoles polytechniques – demeure largement soustraite à la sphère d'influence de la Confédération⁵⁵. L'article 69 cst. qui donne à la Confédération la compétence de prendre des mesures destinées à lutter contre les maladies transmissibles, les maladies très répandues et les maladies particulièrement dangereuses, lui non plus, n'offre pas une base constitutionnelle permettant d'imposer des règles fédérales de protection de données aux cantons: seule une partie des projets de recherche concernent ces catégories de maladies.

Toutefois, une réglementation uniforme sur la protection des données dans le domaine de la recherche médicale peut se fonder dans sa majeure partie sur l'article 64^{bis} cst., lequel attribue à la Confédération toute compétence en matière de droit pénal. Etant donné qu'il ne s'agit que de réglementer la *communication de données*, il existe une relation matérielle étroite avec le secret professionnel. Selon cet article, la Confédération est compétente pour déterminer les sanctions pénales applicables en cas d'atteinte au secret professionnel, partant, pour réglementer le secret professionnel. Elle a fait usage de cette compétence en édictant l'article 321 du code pénal. Dès lors, du point de vue constitutionnel, rien ne s'oppose à ce que l'on règle de manière précise le secret médical sous l'angle de la protection des données. Il est ainsi admissible, à certaines conditions, de prévoir un nouveau motif justificatif autorisant les atteintes au secret professionnel. Ce motif justificatif trouvera application lorsque les données sont utilisées pour la recherche médicale.

Il en irait toutefois différemment si l'on entendait réglementer également la *collecte et le traitement* de données. Contrairement à la communication de données, ces deux cas ne concernent pas nécessairement le secret professionnel. Si l'on élaborait des principes pour le traitement de données (p. ex. des règles de conservation de données), et si l'on sanctionnait pénalement les manquements à ces principes, on créerait une nouvelle catégorie d'actes punissables. Vu la diversité des atteintes possibles, il ne faut pas sanctionner l'ensemble de ces manquements aux principes du traitement de données mais uniquement ceux qui sont particulièrement graves, respectivement ceux qui mettent en cause l'application de la protection des données (cf. art. 28 et 29 LPD, ainsi que l'art. 179^{novies} CP). En outre la compétence pénale ne doit pas être la base constitutionnelle déterminante pour l'ensemble de la réglementation du traitement de données dans la recherche médicale. En conformité avec ses attributions pénales, la Confédération peut, par contre, édicter des règles d'organisation relatives à une commission d'experts qui aurait pour tâche d'examiner les projets de recherche sous l'angle de la protection des données. Vu que l'administration de la justice pénale est une tâche en principe réservée aux cantons, la Confédération n'a pas, jusqu'à présent, fait usage de ses compétences pénales pour instituer des organes de ce genre. Reste que si des mesures d'organisation sont nécessaires pour qu'une réglementation matérielle du code pénal soit appliquée correctement et conformément au principe de l'égalité de traitement, la Confédération est en droit d'édicter les normes correspondantes⁵⁶. En plus, la commission d'experts ne fonctionnera pas comme un véritable organe de l'administration de la justice pénale, elle jugera uniquement de la nécessité d'autoriser la levée du secret

professionnel dans le cas d'espèce; à ce titre également, on peut affirmer que la commission dont la création est proposée ne remet pas en cause la répartition des compétences.

222.42 Projet de réglementation en général

Il apparaît en outre tout-à-fait défendable de limiter la réglementation à la communication des données. Car c'est lors de communications de données qu'il faut déterminer à quelles conditions il est possible de dévoiler un secret professionnel relatif à des données médicales. En comparaison, il apparaît moins urgent – bien qu'également souhaitable – de réglementer le traitement de données médicales acquises par d'autres moyens que la levée du secret professionnel, notamment lors de communications de dossiers médicaux par des médecins traitants. La raison principale en est que ces traitements seront soumis – du moins tant que les recherches sont exécutées par des institutions de la Confédération ou par des centres de recherche privés – à la loi sur la protection des données. Quant aux hôpitaux cantonaux et universitaires, ils sont soumis, le cas échéant, au droit cantonal sur la protection des données en vigueur. Dans cette situation juridique, la réglementation proposée devrait, dans l'ensemble, conduire à une amélioration sensible de la protection des données médicales.

L'article 19 du projet de loi fédérale sur la protection des données professionnelles renferme une disposition qui privilégie les traitements de données personnelles à des fins ne se rapportant pas à des personnes, notamment à des fins de recherche, de statistique ou de planification. Ainsi, les conditions mises à la communication de données à des tiers seront moins restrictives. Ces dispositions réserveront cependant d'éventuelles obligations de garder le secret. Lorsque la recherche entre en conflit avec un secret professionnel, les dispositions spéciales de la loi sur la protection des données privilégiant certaines formes de traitement ne s'appliqueront pas. Dans ce cas, seul l'article 321^{bis} du code pénal trouvera application.

222.43 Commentaires concernant l'article 321^{bis} CP, ainsi que l'article 26, 3^e alinéa, et 27, 1^{er} alinéa, lettre c, LPD

Article 321^{bis} CP Secret professionnel en matière de recherche médicale

1^{er} alinéa Nouveau motif justificatif pour la levée du secret professionnel

Les motifs justifiant la violation du secret professionnel qui sont mentionnés à l'article 321 CP sont complétés par un nouveau motif justificatif: l'autorisation de lever le secret professionnel donnée par une commission d'experts. Cette autorisation n'est cependant valable que pour la recherche dans le domaine de la médecine ou de la santé publique. Il s'agit en premier lieu de la recherche destinée à combattre efficacement les affections graves ou répandues. Dans le domaine de la santé publique, on exécute également des projets de recherche dont l'intérêt public est incontestable. Les enquêtes sur l'état de santé de la population forment, par exemple, la base indispensable à une planification sérieuse des

besoins hospitaliers. Il doit également être possible de dépister d'éventuels effets secondaires graves de certains médicaments, ainsi que de constituer une documentation scientifique et statistique sur les effets à long terme de certaines thérapies. En revanche, la commission d'experts ne doit pas lever l'obligation du secret pour permettre de simples études de marché.

La loi se contente de définir en termes généraux à quel titre une autorisation de lever le secret professionnel peut être donnée. Il appartiendra à la commission d'experts d'élaborer des critères plus précis. Le nouveau motif justificatif concernera principalement les médecins, les dentistes, ainsi que leur personnel auxiliaire; dans certains cas, les pharmaciens et les sages-femmes pourront également s'en prévaloir; il n'aura par contre guère de signification pour les autres personnes soumises à l'obligation de garder le secret selon l'article 321 du code pénal.

- Un secret professionnel, au sens de l'article 321 du code pénal, subsiste en principe également après la mort du maître du secret⁵⁷. La personne soumise au secret professionnel qui le viole après la mort du maître du secret reste, en l'absence d'une plainte, en principe impunie (art. 28 CP)⁵⁸. Cependant, l'autorisation de la commission d'experts concerne également les données relatives à des personnes décédées, car une violation illicite, par exemple du secret médical, peut également avoir des conséquences disciplinaires, civiles et, exceptionnellement, pénales.

Hormis l'intéressé, seule la commission d'experts est habilitée à donner une autorisation de lever le secret professionnel en faveur de la recherche médicale. La disposition institue une réglementation de droit fédéral complète, qui en tant que réglementation spéciale prime l'article 321, chiffre 2, du code pénal. Selon cette disposition, l'autorité supérieure ou l'autorité de surveillance est également en mesure de délivrer une autorisation de lever le secret professionnel.

Même dans les cas où la commission d'experts pourrait délivrer une autorisation ou l'a déjà délivrée, l'opposition de l'intéressé doit être respectée. Un secret professionnel, notamment un secret médical, ne doit pas être levé contre la volonté expresse de l'intéressé. Si, sur la base d'une autorisation de la commission d'experts, un médecin communique des données personnelles et que par la suite l'intéressé s'y oppose, les chercheurs ne doivent plus travailler avec ces données.

Selon l'article 29 du projet de loi sur la protection des données toute personne qui exerce une activité professionnelle nécessitant la connaissance de données personnelles secrètes et sensibles et qui révèle, sans autorisation, ces données à des tiers, pourra être punie. A l'instar du consentement de l'intéressé, l'autorisation de la commission d'experts permet de révéler de telles données: les éléments constitutifs de cette nouvelle infraction n'étant alors pas réunis, la communication serait justifiée.

2^e alinéa Conditions pour l'obtention de l'autorisation de la commission d'experts

Certaines conditions cumulatives doivent être remplies pour obtenir une autorisation de la commission d'experts levant le secret professionnel.

L'autorisation ne doit être octroyée que si la recherche ne peut être effectuée avec des données rendues anonymes (let. a). Si un projet de recherche peut être

exécuté avec des données ne permettant pas d'identifier la personne concernée, la commission d'experts ne doit pas autoriser la levée du secret professionnel. L'autorisation de la commission d'experts ne peut en outre être donnée que s'il est impossible ou particulièrement difficile d'obtenir le consentement de l'intéressé (let. b). De telles difficultés pourraient avant tout surgir lors de recherches rétrospectives. Ce pourrait également être le cas lorsque les patients concernés par un projet de recherche d'une importante clinique résident sur un vaste territoire, voire même dans plusieurs pays. Les obstacles ne doivent pas être de nature absolue. Il suffit que l'obtention du consentement des personnes concernées exige un effort disproportionné, effort qui mettrait le projet en échec. En pareille occurrence, il appartiendra à la commission d'experts de délimiter plus précisément les frontières. Finalement, il faut au surplus que les intérêts de la recherche priment les intérêts au maintien du secret (let. c).

Ainsi, le projet de recherche, au profit duquel le secret professionnel sera levé, doit répondre à certaines exigences qualitatives. Il appartient à la commission d'experts d'évaluer et de peser les circonstances concrètes dans le cas d'espèce. Elle devra notamment déterminer, si le chercheur est dépendant de l'accès aux données qui l'intéressent, si le projet de recherche est susceptible de favoriser le traitement et d'apporter un progrès médical, si les résultats de la recherche peuvent être utiles à un nombre important de personnes ou encore quelle valeur le projet revêt pour la santé publique. Des règles générales plus étendues ne sont par contre pas de mise. Il est bien évident toutefois que les projets de recherche qui sont une fin en soi ou qui répondent exclusivement à des considérations de politique commerciale ne remplissent assurément pas ces exigences.

3^e alinéa Charges garantissant la protection des données et publication de l'autorisation

La commission d'experts grèvera l'autorisation de charges afin de garantir la protection des données. L'ordonnance d'exécution du Conseil fédéral (5^e al.) précisera ces charges. Il pourra s'agir, par exemple, de charges limitant les buts dans lesquels les données peuvent être communiquées, ou précisant la nature et l'étendue des données, les personnes qui sont délivrées du secret professionnel, la forme de l'utilisation des données, ainsi que le cercle des personnes ayant accès aux données.

En publiant les autorisations délivrées par la commission d'experts, on attirera l'attention des personnes concernées sur les communications prévues. Ainsi, sur la base de cette publication, l'intéressé aura encore une fois la possibilité, par exemple, d'interdire à son médecin de communiquer ses données médicales.

4^e alinéa Autorisation générale et autres simplifications

Le 4^e alinéa attribue à la commission d'experts la compétence d'octroyer des *autorisations générales* lorsque les intérêts légitimes des personnes concernées ne sont pas compromis et que les données personnelles sont rendues anonymes dès le début des recherches. Au premier plan figure la nécessité des cliniques et des instituts médicaux-universitaires d'utiliser les données collectées pour les besoins des soins médicaux à des fins de recherche interne, notamment pour la formation et le perfectionnement du personnel. A cet égard, il y a lieu d'accorder un droit

d'accès aux dossiers médicaux concernant les patients d'autres divisions hospitalières. Dans de tels cas, qui sont en principe soumis au secret professionnel institué par l'article 321 du code pénal, la commission d'experts doit être en mesure d'octroyer une autorisation générale non pas à la personne effectivement soumise au secret, mais à la direction de la clinique ou de l'institut. L'ordonnance d'exécution du Conseil fédéral règlera les modalités. Dès que l'identité de la personne concernée est nécessaire non seulement pour la collecte des données mais aussi pour la suite du traitement, une autorisation doit être demandée à la commission d'experts selon la procédure ordinaire.

L'ordonnance du Conseil fédéral prévoira probablement que les autorisations générales en faveur des cliniques ou des instituts vaudront non seulement pour les chercheurs employés par ces établissements, mais encore pour les candidats au doctorat. Ainsi, ces derniers pourraient avoir accès aux dossiers médicaux aux conditions énoncées – pas de danger pour les intérêts de la personne concernée et anonymisation immédiate – sans violer le secret médical. L'autorisation générale pourrait alors être complétée par un devoir de déclaration des projets de recherche particuliers, afin que la commission d'experts puisse examiner si le cadre de l'autorisation générale est respecté.

Une simplification de la procédure d'autorisation s'impose aussi pour les *registres* médicaux, notamment les registres du cancer. Le Conseil fédéral peut également, sur la base du 4^e alinéa, prévoir pour ces cas une autorisation générale. Ainsi, une telle autorisation pourrait par avance être octroyée à l'organe responsable du registre pour qu'il puisse recevoir communication de données non anonymisées. La commission d'experts devrait assortir cette autorisation de charges, concernant en particulier le chiffage et la conservation des données non anonymisées, et déterminer le cercle des personnes pouvant accéder à des données.

Sur la base du 4^e alinéa le Conseil fédéral peut aussi prévoir une procédure simplifiée dans d'autres cas. Il pourrait, par exemple, pour des cas manifestes, prévoir une procédure de décision présidentielle ou laisser une sous-commission décider.

La loi laisse, à dessein, la porte ouverte à différentes possibilités de simplification. Comme il est difficile d'estimer combien de demandes seront adressées annuellement à la commission d'experts et quelle nature elles revêtiront, une certaine souplesse s'impose. La première année sera une phase d'essai au cours de laquelle la commission d'experts devra pouvoir tester diverses formes d'organisation aux fins d'adopter la plus appropriée.

5^e alinéa Organisation de la commission d'experts et procédure

La commission d'experts sera nommée par le Conseil fédéral. Elle sera une *autorité fédérale*. Le projet renonce à prévoir des instances cantonales de décision. Une telle solution, serait certes en harmonie avec la structure fédéraliste du pays, mais serait difficilement praticable et présenterait de notables inconvénients. Ainsi la compétence d'autoriser la levée du secret professionnel n'appartiendrait pas uniquement au canton dans lequel la recherche est conduite, mais également aux cantons dans lesquels les données doivent être collectées, voire dans ceux où les intéressés ont leur domicile. Un seul et même projet de recherche d'une clinique universitaire touchant un vaste territoire devrait être soumis, selon les

circonstances, à plusieurs commissions cantonales pour une seule et même autorisation. Cette solution serait impraticable même si chaque canton disposait du personnel nécessaire à la constitution d'une telle commission. En outre, il n'est pas à exclure que différentes commissions, du moins en ce qui concerne les modalités de l'autorisation, parviennent à des conclusions différentes. Il s'ensuivrait une paralysie du travail de recherche et une insécurité juridique. La réglementation proposée laisse cependant ouverte la possibilité de diviser la commission d'experts en sous-commissions, compétentes chacune pour une partie du pays ou pour une région linguistique. Les expériences pratiques de la commission montreront si une solution fédéraliste peut être réalisée par cette voie.

L'autorisation de la commission d'experts doit être demandée indépendamment de toute autre procédure en relation avec un projet de recherche, par exemple une procédure devant le Fonds national ou une commission d'éthique. Cependant, afin d'éviter des retards, la procédure d'autorisation devant la commission d'experts pourra se dérouler parallèlement à d'autres procédures.

L'organisation de la commission d'experts doit être réglée dans une ordonnance du Conseil fédéral. La composition de la commission revêt une importance particulière. Il va de soi qu'elle doit être constituée de membres indépendants et que les besoins de la recherche médicale et les intérêts aussi bien des médecins que des personnes concernées, notamment des patients, doivent être représentés d'une manière paritaire. En outre certains membres de la commission devront avoir une pratique judiciaire.

La procédure devant la commission d'experts sera réglée en principe par la loi fédérale sur la procédure administrative. L'ordonnance d'exécution du Conseil fédéral devrait en outre déterminer quelles informations doivent figurer dans la demande d'autorisation.

La commission d'experts délibérera sans instructions. Elle sera rattachée administrativement au Département fédéral de l'intérieur. Le secrétariat devrait être confié à l'Office fédéral de la santé publique.

6^e alinéa Secret de la recherche

Toute personne qui, à des fins de recherche dans le domaine médical ou de la santé publique, traite des informations soumises au secret professionnel doit être soumise à l'obligation de garder le secret. Il importe donc que les destinataires des informations, c'est-à-dire les chercheurs et les auxiliaires qui obtiennent du médecin traitant, grâce à la levée du secret de fonction, des données personnelles, se voient également imposer l'obligation de garder le secret. Lorsqu'une autorité prend une décision autorisant la levée du secret de fonction au profit d'un chercheur, indépendamment du consentement des intéressés, il faut s'assurer qu'aucun tiers non autorisé n'obtienne communication des informations. S'agissant du contenu de l'obligation de garder le secret imposée au chercheur, aucune distinction n'est faite entre les informations que les médecins ont communiquées en se fondant sur la décision de la commission d'experts et celles qu'ils ont révélées avec le consentement de l'intéressé. Dans les deux cas en effet, l'utilisation de données personnelles dans la recherche augmente de manière substan-

tielle le risque d'autres divulgations. Par ailleurs, une telle distinction serait difficilement applicable dans la pratique.

Ainsi, le 6^e alinéa élargit le cercle des personnes soumises à l'article 321 CP. Parallèlement, le nouveau motif justificatif s'applique également à ces nouveaux détenteurs du secret professionnel que sont les chercheurs. Sous réserve du consentement de la personne concernée ou de l'autorisation de la commission d'experts, ceux-ci pourront à leur tour transmettre les données médicales à d'autres chercheurs.

Dans la mesure où les chercheurs collectent les données pour leurs projets de recherche directement auprès des intéressés et indépendamment, par exemple, d'un traitement médical, il n'apparaît pas justifié de les soumettre à un secret professionnel correspondant. Il n'existe pas en effet entre le chercheur et la personne qui le renseigne ce rapport de confiance qui lie le médecin à son patient. On appliquera dès lors dans ce cas la disposition concernant la violation du devoir de discrétion (art. 29 LPD).

Article 26, 3^e alinéa, LPD Préposé fédéral à la protection des données

En tant que principal responsable de la mise en œuvre de la protection des données, le préposé est, dans une certaine mesure, prédestiné à jouer le rôle de conseiller de la commission d'experts. Il peut aussi contribuer à assurer une certaine «unité de doctrine» entre la protection des données en général et la protection des données dans la recherche médicale. Enfin, il doit assumer là aussi une fonction de contrôle. Le préposé fédéral à la protection des données a, dans la mesure où ses fonctions de conseil et de contrôle l'exigent, un droit d'accès aux informations et aux documents égal à celui dont il dispose en vertu de l'article 24, 3^e alinéa, de la loi fédérale sur la protection des données. Au demeurant, l'ordonnance d'exécution devra régler en détail les mesures de contrôle, en particulier la collaboration entre la commission d'experts et le préposé à la protection des données: la commission d'experts devra informer le préposé à la protection des données des autorisations qu'elle accorde et des charges dont elles sont assorties. Si le préposé à la protection des données constate que ces charges ne sont pas respectées, il doit, à son tour, en avertir la commission d'experts. En outre, l'ordonnance d'exécution peut prévoir que, dans de tels cas, le président enjoint au requérant de se conformer aux charges accompagnant la décision d'autorisation, sous peine de révocation de l'autorisation. Au surplus, il est aussi envisageable d'assortir la décision d'une menace de peine (art. 292 CP).

Enfin, le préposé fédéral à la protection des données doit pouvoir recourir devant la Commission fédérale de la protection des données contre les décisions de la commission d'experts. Il aura ainsi la possibilité de défendre les intérêts de la personne concernée devant cette commission. Il n'apparaît par contre pas nécessaire de reconnaître au préposé la qualité pour agir par la voie du recours de droit administratif devant le Tribunal fédéral.

Article 27, 1^{er} alinéa, lettre c, LPD Voies de droit

Le recours de droit administratif n'est pas directement ouvert contre les décisions de la commission d'experts; afin de décharger le Tribunal fédéral, l'affaire devra

d'abord être portée devant une commission de recours. Cette solution s'impose pour deux raisons. D'abord elle est dans la ligne de la révision de la loi fédérale d'organisation judiciaire; ensuite, la loi fédérale sur la protection des données personnelles institue elle aussi, une commission spéciale de recours pour le domaine de la protection des données: la Commission fédérale de la protection des données.

222.5 Modifications de la loi fédérale sur la procédure pénale

Aux termes de son article 2, 2^e alinéa, lettre e, la loi sur la protection des données ne s'applique pas aux traitements de données effectués dans le cadre d'une procédure pénale; à cet égard, les procédures relevant de la loi fédérale du 15 juin 1934 sur la procédure pénale (PPF) sont tout particulièrement visées. En effet, comme nous l'avons vu, la procédure fédérale contient déjà des dispositions spécifiques assurant à la personne concernée des garanties sur la manière dont ces données seront recueillies, utilisées ou communiquées (cf. p. ex. les dispositions sur l'interrogatoire de l'inculpé, art. 39 ss PPF). En outre, il importe de régler spécifiquement à chaque stade de la procédure l'information des personnes impliquées. De surcroît, le déroulement de la procédure risquerait d'être compliqué, voir même entravé par une application parallèle de la loi sur la protection des données.

La procédure fédérale a, au cours de ces dernières années, fait l'objet de maintes révisions. Que l'on songe par exemple à l'extension du contrôle judiciaire des actes de procédure pénale. Les principes généraux du droit de procédure sont cependant restés les mêmes au cours de ces 50 dernières années. Il en résulte notamment que les recherches de police judiciaire ne font pas l'objet de dispositions spécifiques de protection des données. Cette lacune doit être comblée, car les informations de police contiennent le plus souvent des données sensibles. Nous vous suggérons donc d'insérer dans la loi fédérale sur la procédure pénale quelques normes sur l'entraide judiciaire, sur la collecte des données de police, sur leur communication et leur destruction, de même que de faire bénéficier la personne concernée d'un droit d'accès.

A ces dispositions de protection des données, s'ajoute une poignée de *normes relatives à certaines opérations d'instruction qui ont un caractère contraignant*: fouille, examen corporel et prise d'empreintes digitales. Chacune de ces opérations constitue en soi une atteinte; il y a donc lieu de définir à quelles conditions la police judiciaire peut les entreprendre. Il importe en outre d'instituer une voie de recours contre ces opérations devant la Chambre d'accusation du Tribunal fédéral. Si l'on entend se conformer strictement aux exigences de la légalité s'agissant du traitement de données, il n'y a pas de raison de se montrer moins sévère s'agissant des mesures de contrainte. Les dispositions que nous préconisons à cet égard s'inspirent largement des solutions consacrées par certaines lois cantonales.

Désormais, toutes les atteintes sérieuses à la liberté personnelle s'appuieront sur une base légale. Par contre, pour les atteintes légères à la personnalité, la clause générale instituée par l'article 102 de cette loi suffit. Une réserve doit être faite

pour l'utilisation des armes à feu par la police, car il existe à cet égard des règles spéciales⁵⁹⁾.

Enfin, relevons qu'il n'y a pas lieu de compléter la procédure pénale militaire par des dispositions semblables. En effet, dans le domaine du droit pénal militaire, les recherches préliminaires ont d'emblée un caractère judiciaire: la conduite de la procédure est pratiquement dès le début confiée à un juge d'instruction.

Article 26^{bis}

La police judiciaire de la Confédération ne peut pratiquement pas accomplir ses tâches sans la collaboration d'autres services administratifs relevant soit de la Confédération, soit des cantons, soit encore des communes. Dès lors, il sied de réglementer expressément l'entraide que peut solliciter la police judiciaire fédérale. Cette disposition s'inspire largement de l'article 30 de la loi fédérale sur le droit pénal administratif. En tant que loi spéciale, elle prime l'article 16 de la loi sur la protection des données.

Le 1^{er} alinéa met les autorités fédérales de poursuite pénale au bénéfice d'une *obligation générale d'entraide*. Cette obligation incombe à tous les organes fédéraux, de même qu'aux organes cantonaux et communaux. Elle couvre tant la communication de renseignements que la consultation de pièces, à quoi il faut ajouter la remise des documents ou des objets qui peuvent servir de pièces à conviction (cf. art. 65 PPF).

La portée de l'obligation d'entraide n'est cependant pas absolue. Suivant le 2^e alinéa, l'entraide peut être refusée ou restreinte si un intérêt public important ou un intérêt manifestement légitime d'une personne concernée l'exige (let. a), ou encore si le secret professionnel le requiert (let. b). Cette disposition correspond pour l'essentiel à l'article 16, 3^e alinéa, de la loi sur la protection des données.

A l'instar de la disposition équivalente du droit pénal administratif, les organisations chargées de tâches de droit public sont tenues, en vertu du 3^e alinéa de prêter assistance dans la même mesure que les autorités.

Suivant le 4^e alinéa, les différends entre autorités administratives fédérales sont tranchés soit par le département dont relèvent les autorités concernées, soit par le Conseil fédéral, si les autorités concernées ne relèvent pas du même département. Si le différend oppose une autorité fédérale à une autorité cantonale, il appartient à la Chambre d'accusation du Tribunal fédéral de le trancher, comme elle le fait du reste pour les contestations entre autorités cantonales (art. 357 CP et art. 252 PPF). Enfin, dans les rares cas où le différend viendrait à opposer une instance judiciaire à une instance administrative de la Confédération, un échange de vues entre le Conseil fédéral et le Tribunal fédéral règlera le désaccord.

Le 5^e alinéa prévoit l'application subsidiaire des dispositions d'entraide judiciaire que renferment le code pénal et la loi sur l'organisation judiciaire.

Article 52

Etant donné que le nouvel article 105^{bis} règle de manière exhaustive le recours contre les mesures de contrainte, le 2^e alinéa, deuxième phrase de l'article 52, est devenu superflu; par conséquent, il peut être abrogé.

Article 64^{bis}

Cette disposition pose certains principes de protection des données, applicables aux activités des autorités pénales fédérales, y compris les organes de la police judiciaire. Sont ainsi réglées, la collecte, la rectification et la destruction des données. La norme proposée régit toutes les données personnelles, et non les seules données sensibles. Dans le cadre d'une enquête, notamment lorsqu'il s'agit de procéder à un interrogatoire, il est en effet impossible de dissocier les données non-sensibles des données sensibles.

S'inspirant de l'article 15 LPD, le 1^{er} alinéa stipule que, lors des recherches préliminaires, les données ne peuvent être collectées qu'auprès des personnes concernées et de façon reconnaissable. Toutefois, cette règle n'a pas une portée absolue. Pour assurer l'efficacité d'une enquête pénale, il importe que la police judiciaire soit en droit de déroger à ces principes. Signalons en outre que le terme «*également*» vise à enjoindre aux autorités de ne pas se contenter de recueillir les informations auprès de témoins ou de tiers, mais aussi à corroborer les renseignements recueillis avec les déclarations des personnes concernées.

Le 2^e alinéa concrétise un principe général de la protection des données posé par l'article 4, 2^e alinéa, LPD: les données doivent être exactes. Ainsi, en cas de rectification ou de destruction, le maître du fichier ou l'organe responsable doit en avertir sans délai l'autorité ou l'organe auquel la donnée a été communiquée. Si cette prescription a trouvé place parmi les dispositions générales, c'est parce qu'il importe de montrer clairement qu'elle est applicable à *toutes les phases de la procédure pénale fédérale*.

Le 3^e alinéa régit les données qui ne sont plus nécessaires à la conduite de l'instruction; en ce sens, il est le pendant de l'article 66, alinéa 1^{er}, de la loi fédérale sur la procédure pénale, qui dispose que les enregistrements d'écoutes téléphoniques dépourvus d'utilité doivent être détruits à l'issue de la procédure. Le 3^e alinéa précise toutefois que les données qui peuvent être utilisées dans le cadre d'une autre procédure peuvent être conservées; cependant, leur utilisation est soumise à certaines conditions posées par la jurisprudence⁶⁰). Relevons enfin que le dossier constitué à l'occasion des recherches préliminaires sera, pour le cas où celles-ci conduisent à l'ouverture d'une procédure formelle, détruit ou versé aux archives à l'issue de la procédure pénale fédérale ou cantonale, (cf. le nouvel art. 107^{bis}).

Article 72^{bis}

Cette disposition régit la surveillance de manifestations. A cet égard, une question est depuis longtemps controversée: dans quelle mesure la police est-elle en droit de filmer ou de photographier une manifestation se déroulant dans la légalité? Ces prises de vues sont au regard de la protection des données discutables, car elles sont le révélateur des activités politiques des participants à la manifestation. Suivant notre proposition, la police ne sera désormais en droit de filmer ou de photographier une manifestation se déroulant dans la légalité que si les participants en viennent à commettre des infractions ou, s'il ressort effectivement des circonstances, que ces personnes envisagent d'en commettre. Cette dernière condition sera remplie lorsque, par exemple, les manifestants portent des armes

ou des outils dangereux, ou lorsque, avant la manifestation, des appels à commettre des actes de violence ont été lancés.

Il y a lieu de signaler que nous avons renoncé à réglementer semblablement l'utilisation d'*appareils acoustiques*. En effet, ceux qui prennent la parole lors de manifestations s'affichent publiquement en toute connaissance de cause.

Relevons enfin que nous avons aussi renoncé à réglementer la *surveillance traditionnelle de personnes*, notamment la *filature*. Il va de soi que l'on ne saurait mettre sous surveillance une personne que si de forts soupçons pèsent sur elle. D'ailleurs, cette compétence est inhérente à la mission générale de la police de prévenir et de découvrir les délits. On doit néanmoins convenir que s'il est vrai que les opérations de surveillance intensive portent sérieusement atteinte à la personnalité, il n'en demeure pas moins qu'elles sont rares; de surcroît, elles requièrent des moyens techniques qui ne peuvent être mis en œuvre sans l'autorisation du président de la Chambre d'accusation (art. 66 ss PPF). Dès lors il nous paraît superflu de créer une norme spéciale réglant la surveillance et la filature des personnes.

Article 73^{bis}

Jusqu'à ce jour, seule la disposition sur la perquisition traite de la fouille des personnes, et encore n'est-ce qu'en passant (art. 67, 1^{er} al., deuxième phrase, PPF). Au reste, la police judiciaire en est réduite à se fonder sur la clause générale de l'article 102 de la loi fédérale sur la procédure pénale, une disposition qui l'habilite à relever les traces des infractions et de veiller à leur conservation. On ne saurait toutefois méconnaître que la fouille peut être une atteinte significative à la liberté personnelle; dès lors, une base légale expresse s'impose.

Le 1^{er} alinéa définit à quelles conditions la police peut fouiller une personne. Ainsi, la fouille est licite à chaque fois que les conditions pour appréhender une personne sont réunies (let. a); tel est le cas lorsqu'un mandat d'arrêt a été délivré ou s'il y a péril en la demeure (art. 44 et 62 PPF). En outre, une personne peut être fouillée, si elle est soupçonnée de détenir des objets qui doivent être mis en sûreté (let. b), notamment qui doivent être confisqués⁶¹⁾ ou séquestrés. Enfin, il peut être procédé à une fouille aux fins d'identification (let. c) ou dans le but de protéger une personne qui n'a plus la jouissance de ses facultés mentales (let. d).

Suivant le 2^e alinéa une personne peut aussi être fouillée, si la protection des agents de la police ou de tiers est en jeu. Cette disposition vise tout particulièrement la protection, imposée par le droit international, des chefs d'Etat, des membres de gouvernements et des diplomates en visite officielle ou participant à une conférence internationale.

On relèvera enfin que la teneur du 3^e alinéa est semblable à celle de l'article 48, 2^e alinéa, de la loi sur le droit pénal administratif (RS 313.0), disposition qui prévoit que la fouille ne doit être opérée que par une personne de même sexe ou par un médecin. Il peut toutefois être fait exception à cette règle si un dommage irréparable risque de se produire.

Article 73^{ter}

Cette disposition définit à quelles conditions une personne peut être soumise à un examen physique ou psychique au cours de l'enquête. Inutile de préciser que pareils examens constituent une atteinte grave à la personnalité de la personne concernée. Dès lors, le 1^{er} alinéa ne les autorise que s'ils sont nécessaires à l'établissement des faits (let. a), ou s'ils sont le seul moyen de déterminer si la personne inculpée est capable de discernement, apte à participer aux débats ou à supporter une détention (let. b).

Le 2^e alinéa attribue au seul procureur général la compétence d'ordonner un examen physique ou psychique au cours des recherches préliminaires.

Suivant le 3^e alinéa l'examen physique ou psychique d'une personne *non inculpée* est soumis à un régime juridique plus sévère. Celle-ci ne peut être examinée contre son gré que s'il s'agit d'élucider un fait essentiel qui ne peut l'être par un autre moyen. A l'instar de ce que prévoient certaines procédures cantonales, toute personne qui est en droit de refuser de témoigner est également en *droit de s'opposer de façon absolue* à son examen physique ou psychique.

Suivant le 4^e alinéa l'examen ne peut être confié qu'à une personne qualifiée. Cet alinéa souligne en outre qu'«une atteinte à l'intégrité corporelle n'est licite qui si tout risque de préjudice est écarté».

Le 5^e alinéa attribue à la police judiciaire la compétence d'ordonner une prise de sang en cas de forts soupçons. On notera enfin que des auxiliaires qualifiés peuvent également procéder à ces opérations.

Article 73^{quater}

Les mesures d'identification et de comparaison font partie des moyens classiques à disposition de la police pour lutter contre la criminalité. D'ordinaire, on range parmi les mesures d'identification le fait de prendre les empreintes digitales, le relevé des traces de délits, les photographies et les signalements⁶²⁾; à ces mesures s'ajouteront d'autres mesures d'identification au fur et à mesure des progrès enregistrés dans le domaine de la police scientifique. On songera tout particulièrement aux nouvelles techniques de comparaison de la voix ou des cheveux.

Le nouvel article 73^{quater}, qui s'inscrit dans la ligne de l'article 30, 4^e alinéa, lettre c, LPD, fournit la base légale nécessaire à la mise en œuvre de ces moyens d'investigation de première importance⁶³⁾. Peuvent être soumis à des mesures d'identification, premièrement un inculpé, si l'administration des preuves l'exige (let. a), secondement, toute autre personne, s'il se révèle nécessaire de déterminer l'origine de traces (let. b). Les empreintes des personnes acquittées et celles prises sur d'autres personnes pour constater leur droit à accéder au lieu du délit sont détruites conformément aux dispositions pertinentes de l'ordonnance sur le service d'identification. Quant aux autres pièces, elles seront à leur tour détruites passé un certain délai⁶⁴⁾. Il n'y a pas lieu de réglementer spécifiquement l'obtention, aux fins de comparaison, de spécimens d'écriture ou de la voix; en effet, l'article 102 de la loi fédérale sur la procédure pénale fournit à cet égard une base légale suffisante, du moment qu'il est, en pratique, difficilement possible de contraindre une personne à fournir ces spécimens contre sa volonté.

Article 101^{bis}

Seul un juge d'instruction peut procéder à une audition de témoins au sens strict. Cela dit, la police judiciaire peut, lors des recherches préliminaires, entendre des tiers à titre de renseignement⁶⁵⁾, pour autant que ceux-ci ne puissent pas se prévaloir du droit de refuser le témoignage. L'article 101^{bis}, qui est calqué sur l'article 40 de la loi sur le droit pénal administratif (RS 313.10), ne fait que consacrer cette pratique dans la loi. Il est ainsi expressément dit que la police judiciaire est tenue d'aviser toute personne en droit de refuser son témoignage lors de l'instruction préparatoire qu'elle n'est pas obligée non plus de répondre lors de la procédure des recherches préliminaires.

Article 102^{bis}

A l'instar de la loi sur la protection des données, le 1^{er} alinéa accorde à tout-un-chacun le droit d'accéder aux données que la police judiciaire a recueillies sur son compte; la requête doit être adressée à celui qui dirige les recherches de la police judiciaire, le procureur général de la Confédération.

Suivant le 2^e alinéa, les renseignements demandés peuvent être restreints ou refusés si leur octroi compromet les recherches (let. a), si des intérêts publics prépondérants, en particulier la sûreté intérieure ou extérieure de la Confédération l'exigent (let. b), ou si des intérêts prépondérants de tiers l'exigent (let. c). Les restrictions au droit d'accès sont en conséquence presque les mêmes que celles prévues par l'article 6 de la loi sur la protection des données. Il importe en effet qu'un délinquant ne tire pas parti de son droit d'accès pour savoir si la police est sur ses traces. Même dans le domaine des recherches de la police judiciaire, le requérant qui s'est vu refuser ou restreindre l'accès n'est pas dépourvu de moyens juridiques: il peut saisir le préposé fédéral à la protection des données (cf. nos remarques concernant l'art. 102^{1er}):

Le 3^e alinéa concrétise une exigence de la protection des données: la personne concernée a droit à ce qu'aucune donnée inexacte ne soit traitée à son sujet. Reste que la portée du qualificatif «inexact» doit être relativisée: il n'y a pas lieu de procéder à la rectification ou à la destruction d'une donnée dont l'exactitude n'a pas été formellement établie. Toutes les informations qui sont recueillies au stade de l'enquête préliminaire, le sont en vue de leur appréciation future par un juge, lequel sera appelé à déterminer ce qui est «vrai» et ce qui est «faux». Il s'ensuit qu'il n'est pas toujours possible, au stade de l'enquête préliminaire déjà, de procéder à une rectification au sens du droit de la protection des données. En revanche, le 3^e alinéa impose la rectification de données qui sont traitées comme si leur exactitude avait été prouvée, alors même que la preuve n'a pas encore été fournie. Relevons enfin que dans la pratique on ne doit pas se montrer trop sévère quant à l'*appréciation de l'intérêt légitime* du requérant. Reste que ce dernier doit pour le moins rendre vraisemblable un intérêt propre. Au demeurant il va de soi que l'office qui s'apercevrait que des données sont erronées devrait de lui-même procéder à leur rectification ou à leur destruction.

Suivant le 4^e alinéa, il appartient à la police judiciaire d'apporter la preuve de l'exactitude d'une donnée; la personne concernée a en effet rarement les moyens de prouver elle-même l'inexactitude de l'information. Il peut cependant arriver

que ni l'exactitude de la donnée ne puisse être prouvée; dans ce cas, il pourra être fait mention au dossier du caractère litigieux de la donnée. Cette solution, que connaissent déjà les lois sur les données de police des cantons de Vaud et du Valais, est conforme aux principes généraux de la procédure pénale.

Article 102^{ter}

Si le procureur général refuse ou restreint l'accès, le requérant peut, en vertu du 1^{er} alinéa, porter l'affaire devant le préposé fédéral à la protection des données. Celui-ci peut s'informer auprès du procureur général.

Aux termes du 2^e alinéa le préposé peut recommander au procureur général de reconsidérer sa décision, s'il ne parvient pas aux mêmes conclusions que lui.

Le 3^e alinéa vise l'hypothèse où le procureur général n'est pas d'accord avec la recommandation; dans ce cas, le préposé ou le procureur peuvent saisir la Chambre d'accusation du Tribunal fédéral. Cette voie n'est pas nouvelle: le Tribunal fédéral dispose déjà de certaines attributions dans le domaine de l'enquête préliminaire (détention, surveillance officielle, levée des scellés); de surcroît, la présente révision de la loi fédérale sur la procédure pénale entend lui octroyer plus de compétences dans ce domaine. Il y a lieu de relever que, afin de ne pas compromettre l'enquête, la personne concernée n'est pas partie à la procédure. Si nécessaire, la Chambre d'accusation peut consulter le dossier de la police judiciaire.

Article 102^{quater}

Les données de police sont pour la plupart des informations hautement sensibles; il importe dès lors d'en limiter la communication au strict nécessaire. A cet effet, le 1^{er} alinéa dresse, sur le modèle de plusieurs réglementations cantonales, la liste des autorités auxquelles des données recueillies par la police judiciaire peuvent être communiquées.

Quant au 2^e alinéa, il réserve les autres dispositions en matière d'entraide judiciaire. Sont en particulier visés par cette disposition, les articles 352 et suivants du code pénal – qui définissent la procédure d'entraide judiciaire –, et les articles 19 et 30 de la loi fédérale sur le droit pénal administratif – qui obligent les autorités à dénoncer les infractions et à fournir l'entraide judiciaire. Enfin, l'entraide judiciaire en faveur des autorités judiciaires militaires est réglée par les articles 18 et suivants de la procédure pénale militaire (RS 322.1).

Article 105^{bis}

A l'heure actuelle, seules quelques-unes des mesures de contrainte que le procureur général peut ordonner sont soumises au contrôle de la Chambre d'accusation; il s'agit du rejet d'une demande de mise en liberté (art. 52 PPF), de la surveillance de la correspondance postale, téléphonique et télégraphique (art. 66^{bis} PPF) et de la perquisition de papiers (art. 69, 3^e al., PPF). Les autres mesures de contrainte envisageables, tels le séquestre et la perquisition domiciliaire, échappent au contrôle direct des juges fédéraux. A l'instar de la loi fédérale sur le droit pénal administratif (c. art. 26, 1^{er} al., DPA; RS 313.0), le 1^{er} alinéa accorde à la personne concernée le droit de recourir devant la Chambre d'accusation du Tribunal fédéral contre une mesure de contrainte, notamment l'arrestation,

+ l'arrestation provisoire, le séquestre, l'examen médical, la fouille et la confiscation. Cela ne signifie cependant pas que la Chambre d'accusation doit substituer son appréciation à celle du juge d'instruction, ni qu'elle doit contrôler l'opportunité de chaque mesure d'instruction. Il n'y a pas lieu de modifier la pratique de la Chambre d'accusation⁶⁶⁾ à cet égard.

Quant aux opérations de la police judiciaire qui portent une atteinte moindre au droit de la personnalité, elles peuvent faire l'objet d'une dénonciation à l'autorité de surveillance, en l'occurrence le Département fédéral de justice et police (cf. art. 17, 1^{er} al., PPF).

Article 107^{bis}

Suivant le 1^{er} *alinéa* le Ministère public de la Confédération doit détruire ou archiver les pièces à l'issue de la procédure fédérale ou cantonale. Ce principe doit toutefois être tempéré s'agissant des recherches préliminaires de la police judiciaire. Souvent, les actes doivent être conservés en vue d'une éventuelle demande de révision ou d'une action en dommages-intérêts⁶⁷⁾. On relèvera également que les documents peuvent être nécessaires pour établir des statistiques. Il importe en outre de pouvoir conserver, traiter et dépouiller sur une longue période les informations recueillies à l'occasion d'opérations de renseignement à long terme ou dans le cadre de la lutte contre le terrorisme; une partie de ces informations sont en effet obtenues lors de recherches préliminaires au sens de la procédure pénale fédérale. La destruction prématurée de ces informations pourrait compromettre la sûreté intérieure ou extérieure de la Confédération. Les prescriptions sur la conservation des documents sont dès lors réservées. Ainsi, le procureur général doit prendre sous sa garde le dossier de l'instruction suspendue (art. 124 PPF). C'est pourquoi le 1^{er} *alinéa* prévoit, pour tous ces cas, la possibilité de verser les dossiers pertinents aux *archives*. Les dispositions régissant les archives fédérales pourront en outre prévoir une obligation de déposer ces dossiers aux Archives fédérales.

Le 2^e *alinéa* restreint les possibilités d'avoir recours aux pièces archivées: celles-ci ne peuvent être utilisées que dans le cadre d'une autre procédure ou pour des traitements ne se rapportant pas à des personnes, par exemple pour l'établissement de statistiques.

Suivant le 3^e *alinéa*, il appartient au Conseil fédéral de préciser les modalités de l'archivage par la voie réglementaire. A cette occasion, il règlera notamment l'organisation de l'archivage.

222.6 Modification de la loi fédérale sur l'entraide internationale en matière pénale

222.61 L'organisation internationale de police criminelle INTERPOL

La présente révision a pour objet de réglementer la coopération entre l'organisation internationale de police criminelle (INTERPOL) et notre pays. Il importe en effet de canaliser un flux transfrontière d'informations policières dont le volume est toujours plus considérable: plus d'une centaine de milliers de ces informations ont transité en 1986 par le Bureau central suisse, l'organe du Ministère public

chargé d'assurer la liaison entre les services de police suisses et étrangers. Il est donc nécessaire de fixer dans la loi sur l'entraide judiciaire le cadre juridique de la coopération avec INTERPOL (compétences et attributions des services fédéraux concernés), et ce, tout en respectant les exigences actuelles de la protection des données. L'accomplissement des tâches et l'efficacité d'INTERPOL n'en souffriront aucunement.

Fondé en 1923, INTERPOL regroupe les polices criminelles de 146 Etats. La Suisse est membre de l'organisation depuis ses débuts. Aux termes de ses statuts, INTERPOL a pour but d'assurer et de développer, dans les limites des accords internationaux et des lois nationales, l'assistance réciproque la plus large possible entre les autorités de police criminelle et, partant, de contribuer efficacement à la prévention et à la répression des infractions.

L'activité d'INTERPOL est avant tout axée sur l'échange d'informations policières entre les différents pays membres (mandats d'arrêts internationaux, avis de recherche, demandes de mise sous surveillance, demandes d'identification, etc.). Ces échanges s'effectuent par l'intermédiaire d'organes de liaison, les Bureaux centraux nationaux. Ceux-ci servent de plaque tournante entre d'une part les différentes autorités de police de chaque pays, d'autre part le Secrétariat général de l'organisation ou les Bureaux centraux nationaux des autres pays membres. La plupart des informations policières entre Bureaux centraux nationaux transitent par le Secrétariat général; les communications directes entre Bureaux centraux nationaux sont toutefois fréquentes. Alors que le premier cas est régi par le «Règlement de 1984 sur le traitement et la communication d'informations dans le cadre d'INTERPOL» (ci-après règlement 84), le second ne fait l'objet d'aucune réglementation de protection des données; toutefois un règlement pertinent est en préparation (cf. art. 11, règlement 84; annexe 2 de l'ordonnance du 1^{er} décembre 1986 concernant le Bureau central national INTERPOL Suisse, OBCN; RS 172.213.56).

222.62 Une réglementation nécessaire

Les échanges internationaux d'informations policières sont aujourd'hui régis par les statuts d'INTERPOL, encore que ceux-ci réservent expressément le droit national des Etats membres. Aucun Bureau central national n'est tenu de transmettre une information si le droit national s'y oppose. Du fait de l'ordonnance du 1^{er} décembre 1986 concernant le Bureau central national INTERPOL Suisse, les statuts d'INTERPOL font partie intégrante de notre ordre juridique; cela dit, on doit convenir que cette ordonnance ne dispose pas d'une base légale suffisante.

La modification qui vous est soumise tend à consolider l'assise juridique nécessaire à la coopération avec INTERPOL. Il s'agit en premier lieu de déterminer à quelles conditions des informations de police peuvent être communiquées en vue de *prévenir* des infractions. La loi fédérale sur l'entraide internationale en matière pénale (EIMP; RS 351.1) ne s'applique qu'à la *poursuite* des infractions pénales; en conséquence, les principes qu'elle renferme, dont certains relèvent partiellement de la protection des données (p. ex. l'interdiction de l'entraide en cas de

4 poursuites en raison d'opinions politiques, de la race, de la religion ou de la nationalité, art. 2 EIMP), ne s'appliquent pas à la prévention des infractions. Puisque le règlement INTERPOL concernant l'échange direct d'informations entre Bureaux centraux nationaux n'est qu'en préparation, il importe de créer le cadre normatif régissant les échanges de données entre le Ministère public de la Confédération, dans sa fonction de Bureau central national, et les Bureaux centraux nationaux des pays étrangers.

Les modifications que nous proposons prennent en compte la spécificité des échanges d'informations de police. Des données ne pourront être transmises en vue de prévenir des infractions que si, *au vu des circonstances réelles, la commission d'un crime ou d'un délit est très probable*. De surcroît, les principes généraux en matière d'entraide judiciaire consacrés par la EIMP deviennent applicables à ce type de communication. Il est en outre prévu que les échanges directs d'informations entre Bureaux centraux nationaux devront se conformer au règlement INTERPOL de 1984 comme à tout autre réglementation future émanant de cette organisation. Ainsi, le droit suisse aussi garantira certains principes de protection des données lors des échanges d'informations dans le cadre d'INTERPOL.

222.63 Emplacement des dispositions proposées

Les échanges internationaux d'informations de police criminelle relèvent en fait et en droit du domaine de l'entraide judiciaire et administrative en matière pénale. Dès lors, le siège des dispositions que nous proposons est la EIMP et non le code pénal.

Les dispositions sur la coopération avec INTERPOL formeront une nouvelle section de l'EIMP. Il sera ainsi clairement établi que ces normes ne visent que la transmission d'informations de police et non les communications de données effectuées dans le cadre d'une procédure d'entraide judiciaire; et même si ces communications empruntent les canaux d'INTERPOL et partant transitent par les Bureaux centraux nationaux (cf. art. 29, 2^e al., EIMP). Relevons enfin que la loi sur la protection des données n'est pas applicable aux demandes d'entraide judiciaire (cf. art. 2, 2^e al., let. f, LPD), car ces demandes sont soumises à des règles de procédure sévères assurant une protection juridique étoffée.

222.64 Commentaire des diverses dispositions

Article 81a Compétences

Aux termes de l'article 32 des statuts d'INTERPOL, chaque pays doit désigner un Bureau central national. Cet organisme public a la tâche d'assurer la liaison entre ses propres autorités de poursuite pénale d'une part, et les Bureaux centraux nationaux d'autres Etats et le secrétariat général d'INTERPOL d'autre part. Le nouvel article 81a répond à cette injonction en désignant, comme le faisait déjà l'article 1^{er} de l'ordonnance concernant le Bureau central national INTERPOL Suisse, le Ministère public de la Confédération en tant que Bureau central national.

Article 81b Attributions

Cette disposition détermine à quelle fin et dans quelle mesure le Ministère public peut coopérer avec le Secrétariat général d'INTERPOL et les Etats membres. Suivant le 1^{er} alinéa, il peut être procédé à des échanges d'informations aux fins de *poursuivre* les infractions ou d'assurer l'*exécution de peines et de mesures*. Le 2^e alinéa n'autorise la transmission d'informations en vue de *prévenir* des infractions que si, au vu des *circonstances réelles*, la commission d'un crime ou d'un délit est très probable. Le 3^e alinéa souligne que le Ministère public de la Confédération peut communiquer des informations par le canal d'INTERPOL en vue de rechercher des personnes disparues ou d'identifier des inconnus. Font partie de cette catégorie d'*informations non criminelles* en particulier les appels urgents destinés à la centrale d'alarme du Touring Club Suisse. Le 4^e alinéa autorise le Ministère public de la Confédération à *transmettre des informations à des particuliers* en vue de prévenir ou d'élucider des infractions. Il importe en effet de pouvoir communiquer des informations relatives à des objets volés, des chèques et des cartes de crédit falsifiés, etc.

Dans ses attributions de Bureau central national, le Ministère public doit se limiter à la *communication* de données; ce que souligne le recours au verbe «transmettre». Dans cette perspective, il lui appartient de contrôler dans tous les cas la licéité d'une demande ou d'une communication de renseignements. En revanche, le Bureau central national n'est pas en droit d'exploiter les données qui transitent par ses services pour mener ses propres recherches.

Article 81c Protection des données

Cette disposition régit la protection des données dans le cadre de la collaboration avec INTERPOL. Elle institue deux régimes différents suivant que l'échange de données porte sur des *informations de police criminelle* ou sur des *informations destinées à des tâches administratives*. Dans le premier cas, ce sont les principes généraux de la EIMP, de même que les statuts et règlement d'INTERPOL qui sont applicables; dans le second cas, la loi sur la protection des données. Solution logique, car, dans cette seconde éventualité, on a très souvent plus à faire à des données relevant d'une procédure juridictionnelle, et partant exceptée du champ d'application de la LPD (cf. art. 2, 2^e al., let. f, LPD).

Le 1^{er} alinéa souligne que les statuts et règlements d'INTERPOL ne sont applicables dans notre pays que si le Conseil fédéral les a expressément déclarés comme tels. Les règlements d'INTERPOL ne sont en effet pas des traités internationaux, mais de simples accords entre organes de police des différents Etats du globe. Ce faisant, ces règlements n'ont pas à être approuvés par le Conseil fédéral et par l'Assemblée fédérale. Vu leur grande importance matérielle, il importe cependant que le Conseil fédéral se prononce expressément sur leur applicabilité dans notre pays. Le cas échéant, ils seront publiés dans le recueil officiel des lois fédérales et, partant, acquerront force obligatoire. On entend également par *échanges d'informations de police criminelle* les échanges d'informations sans rapport avec une demande d'extradition formelle. Les principes généraux de la loi sur l'entraide judiciaire seront désormais aussi applicables à ce genre de flux de données. Cependant, le préposé fédéral à la protection des données ne peut contrôler la conformité des échanges d'informations avec les

principes de l'EIMP et des dispositions de protection des données des règlements INTERPOL que dans la mesure où l'article 26, 2^e alinéa, LPD le lui permet; autrement dit, si le Ministère public de la Confédération y a consenti. Si le préposé constate des manquements, il peut en informer le procureur général et lui faire des propositions quant aux moyens susceptibles d'y remédier. Après en avoir délibéré avec le procureur général, il lui est loisible d'en faire mention dans son rapport d'activités aux Chambres fédérales et au Conseil fédéral. En revanche, il n'est pas en droit, en cas de désaccord avec le procureur général, de porter l'affaire devant la Commission fédérale de la protection des données; en effet, les échanges d'informations de police ne souffrent en général aucun retard.

Le 2^e alinéa constitue la base légale nécessaire aux échanges d'informations de nature administrative. Ceux-ci sont soumis à la loi sur la protection des données, et ce contrairement aux échanges d'informations de nature de pure police criminelle. Il s'ensuit que le préposé fédéral à la protection des données peut exercer pleinement ses attributions; il lui est en particulier possible de saisir la Commission fédérale de la protection des données en cas de traitements litigieux.

Le 3^e alinéa régit les *échanges directs d'informations avec les Bureaux centraux nationaux étrangers*. Ces échanges doivent également respecter les principes généraux de l'EIMP dont il a été fait mention précédemment. En outre, ils ne sont licites que si les Etats destinataires offrent une protection juridique des données couvrant les informations obtenues directement d'un autre Bureau central national, et non par le canal de la centrale INTERPOL. La protection offerte doit être au moins équivalente à celle qui est accordée aux échanges d'informations qui transitent par la centrale INTERPOL. Cela signifie que l'Etat destinataire doit non seulement veiller à la constante exactitude et actualité des données obtenues, mais encore mettre la personne concernée à même de faire détruire ou corriger les données inexactes. Il se peut que le règlement d'INTERPOL concernant les échanges directs entre Bureaux centraux nationaux ait été adopté avant l'entrée en vigueur de l'article 81c. L'échange direct d'informations avec tous les Etats qui seront soumis à ce règlement sera licite.

Article 81d Aides financières et indemnités

Cette disposition crée une base légale expresse pour l'octroi de contributions financières à INTERPOL.

3 Conséquences financières et effets sur l'état du personnel

31 Conséquences pour la Confédération

D'un côté, la mise en œuvre de la loi sur la protection des données occasionnera certains frais, de l'autre elle aura cependant des conséquences financières positives. Dans un cas comme dans l'autre, il n'est pas possible de chiffrer les effets. On ne saurait toutefois nier que, par suite de la législation sur la protection des données, les organes chargés de traiter des données devront supporter des frais supplémentaires, et ce, en raison surtout de l'obligation de contrôler les traitements de façon plus stricte, de prendre des mesures de sécurité plus sévères, d'octroyer des renseignements aux personnes enregistrées et de modifier les

applications informatiques qui ne sont pas conformes aux exigences légales. Dans certains cas, il faudra peut-être aussi accroître l'effectif d'un service. Cela dit, il est incontestable que la nouvelle loi aura pour effet de rendre les activités administratives plus transparentes, d'améliorer la qualité des données et de renforcer la confiance des administrés dans les systèmes d'informations de la Confédération; ce qui aura nécessairement des conséquences financières positives.

La mise sur pied d'*organes de contrôle* n'ira pas non plus sans conséquences financières. A cet égard, il y a lieu de mentionner les salaires qui devront être versés au préposé fédéral à la protection des données et à ses collaborateurs. Soulignons toutefois que le secrétariat du préposé ne devrait occasionner que peu de frais supplémentaires; en effet, il appartiendra à l'actuel service de la protection des données de l'Office fédéral de la justice de s'acquitter de cette nouvelle tâche, à condition qu'il soit quelque peu étoffé. Ce service, qui a été créé en vertu des directives du Conseil fédéral du 16 mars 1981 concernant la protection des données, emploie actuellement cinq collaborateurs, sans compter les secrétaires. Le service de la protection des données est occupé pour moitié principalement à des tâches législatives. Même si celles-ci viendront à diminuer sensiblement, le secrétariat du préposé devra au moins employer une dizaine de personnes; en effet, la loi prévoit l'enregistrement de certains fichiers privés, de même que des contrôles dans le secteur privé comme dans le secteur public. Le coût d'une unité administrative de dix personnes se monte à quelque 850 000 francs par année. Relevons que les membres de la Commission fédérale de la protection des données et ceux de la commission d'experts en matière de recherche médicale seront indemnisés suivant le tarif applicable aux commissions de recours, à quoi s'ajoutera les frais d'exploitation du secrétariat de chaque commission. Trois postes supplémentaires seront vraisemblablement nécessaires pour les secrétariats des commissions: deux pour le secrétariat de la Commission de la protection des données et un pour celui de la Commission du secret professionnel en matière de recherche médicale. Il est impossible de chiffrer exactement le coût annuel total du fonctionnement des deux commissions; il dépend en effet du nombre des affaires que chaque commission sera appelée à traiter. On peut tout au plus mentionner que les frais d'une procédure devant une commission de recours composée de juges occasionnels s'élève à 1500 francs au moins. Quant aux coûts d'une autorisation levant le secret professionnel à des fins de recherche médicale, ils seront certainement inférieurs à cette somme.

32 Conséquences pour les particuliers

Il est incontestable que, du fait de la mise en œuvre de la présente loi, les personnes qui traitent des données à titre privé devront supporter certains frais. Ceux-ci seront occasionnés en majeure partie par l'annonce des fichiers aux fins d'enregistrement, par la déclaration des communications de données à l'étranger et par l'octroi de renseignements aux personnes concernées. Reste que les entreprises bien organisées n'auront guère de difficultés à s'acquitter de ces obligations. Au demeurant, il ne faut pas surestimer le montant de ces frais, en particulier de ceux relatifs au droit d'accès. Comme l'ont démontré les expériences faites à l'étranger, les dépenses occasionnées par l'exercice du droit

+ d'accès sont nullement disproportionnées: non seulement le droit d'accès est une institution relativement peu utilisée, mais encore l'octroi des renseignements est grandement facilité par les techniques informatiques.

4 Programme de la législature

Le projet de loi sur la protection des données a été annoncé dans le programme de la législature 1987-1991 (FF 1988 I 420, ch. 2.17).

5 Constitutionnalisé

Le fondement constitutionnel de la présente loi a fait l'objet d'un commentaire détaillé aux chiffres 12 et 222.41. Nous vous y renvoyons.

6 Délégation de compétence

Les articles 5, 5^e alinéa, 7, 4^e alinéa, 8, 2^e alinéa, 13, 2^e alinéa, 21, 1^{er} alinéa, et 30, 2^e à 6^e alinéas, prévoient des délégations de compétence législative en faveur du Conseil fédéral, qui sortent de l'habituel pouvoir réglementaire de celui-ci. Le développement rapide de l'informatique peut en effet requérir, pour certains types de traitement, la mise en place d'autres réglementations exécutant les dispositions de la loi ou y dérogeant. La plupart des règles nouvelles seront cependant des règles techniques ou administratives. Vous trouverez des explications plus détaillées à ce sujet dans le commentaire des articles correspondants.

7 Relation avec le droit européen

Le présent projet prend déjà en considération, autant pour le secteur privé que pour le secteur public, les exigences posées par la Convention n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Toutefois, pour que notre pays puisse adhérer à cette Convention, il faudrait encore que les cantons soumettent leur secteur public à une loi sur la protection des données. Aussi longtemps que tous les cantons ne rempliront pas les exigences minimales posées par la Convention, la Suisse ne pourra adhérer à celle-ci⁶⁸.

32077

Notes

- ¹⁾ Cf. jugement du Tribunal constitutionnel ouest-allemand du 15 décembre 1983 (Zenzus-Urteil), BVerfGE 65, 43.
- ²⁾ Cf. ATF 44 II 319 ss; cf. aussi ATF 107 Ia 148 ss, ATF 109 Ia 273 ss.
- ³⁾ Cf. ATF 106 Ia 33 ss.
- ⁴⁾ Cf. ATF 107 Ia 52 ss; cf. aussi ATF 108 IV 158 ss.
- ⁵⁾ Cf. p. ex. JAAC 48/II 1984, numéro 21, p. 143 ss, numéro 26, p. 157 ss.
- ⁶⁾ Cf. BVerfGE 65, 43 (voir note 1).
- ⁷⁾ Cf. ATF 97 II 97 ss.
- ⁸⁾ Message du Conseil fédéral du 5 mai 1982 concernant la révision du code civil suisse, FF 1982 II 661 ss, 682.
- ⁹⁾ ATF 97 II 97 ss; cf. également ATF 109 II 353 ss; 62 II 101, 44 II 319.
- ¹⁰⁾ Cf. ATF 107 II 6, 111 II 209 ss; cf. aussi ATF 84 II 573.
- ¹¹⁾ ATF 106 Ia 280; cf. aussi ATF 109 Ia 279 avec les références citées.
- ¹²⁾ Cf. JAAC 48/II 1984, numéro 25, p. 155 ss; ATF 98 Ib 297.
- ¹³⁾ Cf. ATF 113 Ia 10, 101 Ia 18, 109 Ia 296 ss.
- ¹⁴⁾ FF 1981 I 1314, 1983 II 1212, 1986 III 1007.
- ¹⁵⁾ Cf. p. ex. ordonnance du 20 novembre 1985 sur les enquêtes par sondage auprès de la population (microrécensement), RS 431.116; ordonnance du 8 juillet 1981 sur les relevés à titre d'essai destinés à une statistique pénitentiaire, RS 431.341; ordonnance du DFJ du 1^{er} mars 1984 sur les statistiques de l'assurance-accidents, RS 431.835; ordonnance du 18 avril 1984 sur la tenue d'un registre des entreprises et établissements, RS 431.903.
- ¹⁶⁾ Cf. p. ex. Jörg Paul Müller/Stefan Müller, Grundrechte, partie spéciale, Berne 1985, p. 25; Charles-Albert Morand, Problèmes constitutionnels relatifs à la protection de la personnalité à l'égard des banques de données électroniques, dans: Informatique et protection de la personnalité, Fribourg 1981, p. 15 ss.
- ¹⁷⁾ Cf. toutefois ATF 110 Ia 83 ss; 95 I 103 ss.
- ¹⁸⁾ Cf. Jürg Boll, Die Entbindung vom Arzt- und Anwaltsgeheimnis, thèse, Zurich 1983, p. 3; René Russek, Das ärztliche Berufsgeheimnis, thèse, Zurich 1954, p. 42.
- ¹⁹⁾ Cf. Peter Schäfer, Ärztliche Schweigepflicht und Elektronische Datenverarbeitung, thèse, Zurich 1978, p. 29.
- ²⁰⁾ Pour ce qui suit, cf. particulièrement: Conseil de l'Europe, rapport explicatif concernant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg 1981; Organisation de Coopération et de Développement Economique (OCDE), Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, exposé des motifs, Paris 1980.
- ²¹⁾ Cf. Hans Huber, Berner Kommentar, T. I, numéros 105 ss relatifs à l'article 5 CC, p. 514 ss; Raymond Didisheim, La notion du droit civil fédéral, contribution à l'étude de l'article 64 de la constitution, thèse Lausanne 1973, p. 200 ss.
- ²²⁾ BO N 1972 II p. 2127 ss.
- ²³⁾ BO N 1972 II p. 2128.
- ²⁴⁾ Cf. p. ex. les lois sur la protection des données aux Etats-Unis, au Canada, en Israël, en Norvège, en République fédérale d'Allemagne et (dans une certaine mesure) en France.
- ²⁵⁾ Pour la protection de la sphère privée cf. ATF 97 II 100; Jean-Nicolas Druey, Geheimnissphäre des Unternehmens, Bâle et Stuttgart 1977, p. 163/164; Pierre Tercier, Le nouveau droit de la personnalité, Zurich 1984, p. 75 ss. Il faut encore rappeler la protection pénale, notamment celle de l'article 162 (violation du secret de fabrication ou du secret commercial) et de l'article 273 (service de renseignements économiques) CP (RS 311.0), ainsi que

✱ la protection contre la concurrence déloyale par violation de secrets des articles 4, lettre c, et 6, LCD du 19 décembre 1986 (RS 241).

- ²⁶⁾ Jörg Paul Müller/Stefan Müller (cf. note 16); Ulrich Häfelin/Walter Haller, *Schweizerisches Bundesstrafrecht*, Zürich 1984, p. 350.
- ²⁷⁾ Cf. entre autres, Christian Dominici, *La personnalité juridique internationale du CICR*, dans: *Etudes en l'honneur de Jean Pictet*, Genève/La Haye 1984, p. 666; Paul Reuter, *La personnalité juridique internationale du Comité international de la Croix-Rouge*. Ibid., p. 782; cf. aussi FF 1987 I 369 ss, 383.
- ²⁸⁾ Cf. art. 22 de la LF du 7 décembre 1922 concernant le droit d'auteur sur les œuvres littéraires et artistiques (RS 231.1).
- ²⁹⁾ Cf. p. ex. l'art. 42 de la LF sur la procédure de l'Assemblée fédérale ainsi que sur la forme, la publication et l'entrée en vigueur des actes législatifs (loi sur les rapports entre les conseils; RS 171.11); art. 22 ss du règlement du Conseil national (RS 171.13) et art. 17 et 20 s du règlement du Conseil des Etats (RS 171.14).
- ³⁰⁾ Cf. Simitis/Dammann/Mallmann/Reh, *Kommentar zum Bundesdatenschutzgesetz*, Baden-Baden 1967, numéros 14 ss, ad § 2.
- ³¹⁾ ATF 100 Ib 114.
- ³²⁾ Cf. Schnyder/Murer, *Berner Kommentar*, T. II, sect. 3, partie systématique, n° 54.
- ³³⁾ Art. 7, LF sur le droit pénal administratif (RS 313.0).
- ³⁴⁾ ATF 44 II 319 ss; cf. p. ex. art. 179^{bis} ss, CP (RS 311.0).
- ³⁵⁾ ZR 43/1944, n° 217.
- ³⁶⁾ ATF 112 Ia 100, 110 Ia 85, 103 Ia 492, 100 Ia 10.
- ³⁷⁾ De même le message (cf. note 8), p. 683.
- ³⁸⁾ Cf. art. 934 ss CO (RS 220) et l'ordonnance du 7 juin 1937 sur le registre du commerce (RS 221.411).
- ³⁹⁾ Tercier (note 25), n° 682.
- ⁴⁰⁾ Message (cf. note 8), p. 680/681; Tercier (note 25), n° 840 ss.
- ⁴¹⁾ Cf. Tercier (note 25), n° 799 ss.
- ⁴²⁾ ATF 103 II 294, 86 II 18 ss, 73 II 65.
- ⁴³⁾ Erich Richner, *Umfang und Rechte der Freiheitsrechte der Beamten nach schweizerischem Recht*, Argovie 1954, p. 129; Paul Reichlin, *Die Schweigepflicht des Verwaltungsbeamten*, Zurich 1953, p. 21.
- ⁴⁴⁾ Cf. aussi l'article 30 de la LF du 22 mars 1974 sur le droit pénal administratif (RS 313.0).
- ⁴⁵⁾ Cf. ATF 108 Ib 231, 96 IV 183, 87 IV 141, 86 IV 136.
- ⁴⁶⁾ Cf. p. ex. art. 50 LAVS (RS 831.10); art. 102 LAA (RS 832.20); art. 97 LF sur l'assurance-chômage (RS 837.0), ainsi que l'article 125 de l'ordonnance sur l'assurance-accidents (RS 832.202) et l'article 125 de l'ordonnance sur l'assurance-chômage (RS 837.02).
- ⁴⁷⁾ Cf. p. ex. l'ordonnance sur le registre central des étrangers (RS 142.215).
- ⁴⁸⁾ Cf. art. 90 de l'ACF du 9 décembre 1940 sur la perception d'un impôt fédéral direct, (RS 642.11); art. 32 de la LF du 27 juin 1973 sur les droits de timbre (LT; RS 641.10); art. 36 de la LF du 13 octobre 1965 sur l'impôt anticipé (RS 642.21); art. 4, 2^e al., let. c, et art. 7, 2^e al., de l'ACF du 29 juillet 1941 instituant un impôt sur le chiffre d'affaires (RS 641.20).
- ⁴⁹⁾ ACF du 29 avril 1958 concernant le Service de police du Ministère public fédéral (RS 172.213.52) et prescriptions du DFJP du 29 avril 1958 (FF 1958 II 720 s.).
- ⁵⁰⁾ ATF 104 Ib 384, 101 Ib 110; Fritz Gygi, *Bundesverwaltungsrechtspflege*, 2^e éd. révisée, Berne 1983, p. 160 s.
- ⁵¹⁾ FF 1985 II 741 ss, 968 s.
- ⁵²⁾ Cf. art. 20 du code pénal (RS 311.0); ATF 107 IV 193 ss, 207 cons. 3.

- 53) Urs Ch. Nef, Aktuelle Probleme des Personaldatenschutzes im arbeitsrechtlichen Rechtsverhältnis, Zeitschrift für schweizerisches Recht, 92 (I) 1973, p. 357 ss; Bernhard Frei, Der Persönlichkeitsschutz des Arbeitnehmers nach CO art. 328, 1^{er} al. Unter besonderer Berücksichtigung des Personaldatenschutzes, Bern 1982, p. 48 ss; JAAC 48/1984, vol. II, numéro 33, p. 198 ss.
- 54) Cf. message du 10 novembre 1982, FF 1983 I 255 ss.
- 55) FF 1972 I 410.
- 56) Cf. aussi le projet de LF sur la protection de la grossesse et le caractère punissable de son interruption; FF 1977 III 92 ss.
- 57) Cf. Günter Stratenwerth, Schweizerisches Strafrecht, partie spéciale I, 3^e éd., remaniée, Berne 1983, p. 150; Peter Schäfer (note 19), p. 30 ss.
- 58) Sur le droit de porter plainte des parents, cf. ATF 87 IV 105.
- 59) Cf. ATF 94 IV 7, cons. 1.
- 60) ATF 109 Ia 244 ss.
- 61) ATF 74 IV 213.
- 62) Cf. art. 1^{er} de l'ordonnance concernant le Service d'identification du Ministère public de la Confédération, RS 172.213.57.
- 63) Cf. aussi ATF 109 Ia 156.
- 64) Cf. art. 9 et 17 de l'ordonnance concernant le Service d'identification du Ministère public de la Confédération.
- 65) Markus Peter, Ermittlungen nach Bundesstrafprozess, Kriminalstatistik 1973, p. 565; Robert Hauser, Zeitschrift für Schweiz. Strafrecht 1972, p. 137 ss.
- 66) Cf. ATF 96 IV 141; 95 IV 47.
- 67) Cf. ATF 109 IV 63.
- 68) Cf. art. 4 de la Convention n° 108; *supra* chiffre 117.

du

*L'Assemblée fédérale de la Confédération suisse,
vu les articles 31^{bis}, 2^e alinéa, 64 et 85, chiffre 1, de la constitution;
vu le message du Conseil fédéral du 23 mars 1988¹⁾,
arrête:*

Section 1: But, champ d'application et définitions

Article premier But

La présente loi vise à protéger la personnalité et les droits fondamentaux des personnes lors de traitements de données personnelles.

Art. 2 Champ d'application

¹ La présente loi régit les traitements de données personnelles effectués par:

- a. Des personnes privées;
- b. Des organes fédéraux.

² Elle ne s'applique pas:

- a. Aux données traitées par une personne physique pour un usage exclusivement personnel;
- b. Aux données diffusées par des médias à caractère périodique, telles que la presse, la radio et la télévision;
- c. Aux affaires du ressort de l'Assemblée fédérale;
- d. Aux procédures juridictionnelles devant des autorités judiciaires;
- e. Aux procédures pénales;
- f. Aux procédures d'entraide judiciaire internationale concernant des causes civiles ou pénales;
- g. Aux procédures de recours de droit public ni aux procédures de recours administratif;
- h. Aux registres publics relatifs aux rapports juridiques de droit privé.

Art. 3 Définitions

On entend par:

- a. *Données personnelles* (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable;

¹⁾ FF 1988 II 421

- b. *Personne concernée*, la personne physique ou morale au sujet de laquelle des données sont traitées;
- c. *Personne privée*, la personne physique ou morale soumise au droit privé;
- d. *Organe fédéral*, l'autorité ou le service fédéral ainsi que la personne chargée d'une tâche fédérale;
- e. *Données sensibles*, les données personnelles sur:
 - 1. Les opinions ou activités religieuses, philosophiques, politiques ou syndicales,
 - 2. La santé, la sphère intime ou l'appartenance à une race,
 - 3. Des mesures d'aide sociale,
 - 4. Des poursuites ou sanctions pénales et administratives;
- f. *Profil de la personnalité*, un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;
- g. *Traitement*, toute opération relative à des données – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données;
- h. *Communication*, le fait de rendre des données accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant;
- i. *Fichier*, tout ensemble de données dont la structure permet de rechercher les données par personne concernée;
- k. *Maître du fichier*, la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier;
- l. *Participant*, la personne privée ou l'organe fédéral qui est en droit d'introduire les données dans le fichier ou d'y procéder à des mutations.

Section 2: Dispositions générales de protection des données

Art. 4 Principes

¹ Des données personnelles ne peuvent être collectées que par des procédés licites et conformes à la bonne foi.

² Les données doivent être exactes.

³ Tout traitement de données doit être conforme au principe de la proportionnalité.

⁴ Les données ne doivent être traitées que dans le but indiqué lors de leur collecte, prévu par une loi ou ressortant des circonstances.

⁵ Aucune donnée ne peut être communiquée à l'étranger si la personnalité des personnes concernées s'en trouvait gravement menacée, notamment du fait de l'absence d'une protection des données comparable à celle qu'a instituée la Suisse.

⁶ Les données doivent être protégées contre tout traitement non autorisé, par des mesures d'organisation et des mesures techniques appropriées.

Art. 5 Droit d'accès

¹ Toute personne peut demander au maître d'un fichier si des données la concernant sont traitées.

² Le maître du fichier doit lui communiquer:

- a. Toutes les données la concernant qui sont contenues dans le fichier; et
- b. Le but et éventuellement la base juridique du traitement, les catégories de données traitées, de participants au fichier et de destinataires des données.

³ Le maître du fichier peut confier à un médecin le soin de communiquer à la personne concernée des données sur sa santé.

⁴ Le maître du fichier qui fait traiter des données par un tiers demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers, si celui-ci ne communique pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse.

⁵ Les renseignements sont, en règle générale, fournis par écrit et gratuitement. Le Conseil fédéral règle les exceptions. Il peut notamment prévoir un émolument lorsque l'octroi des renseignements occasionne un volume de travail excessif.

⁶ Nul ne peut renoncer par avance au droit d'accès.

Art. 6 Restrictions du droit d'accès

¹ Le maître du fichier peut refuser ou restreindre les renseignements demandés, voire en différer l'octroi, dans la mesure où:

- a. Une loi au sens formel le prévoit;
- b. Un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Confédération, l'exige;
- c. L'octroi des renseignements risque de compromettre une instruction pénale ou une autre procédure d'instruction;
- d. Un intérêt prépondérant du maître du fichier l'exige et celui-ci ne communique pas les données à des tiers; ou
- e. Un intérêt prépondérant d'un tiers l'exige.

² Le maître du fichier doit indiquer pour quel motif il refuse de fournir les renseignements.

Art. 7 Registre des fichiers

¹ Le préposé fédéral à la protection des données tient un registre des fichiers. Toute personne peut consulter le registre.

² Les organes fédéraux sont tenus de déclarer tous leurs fichiers aux fins d'enregistrement auprès du préposé. Les personnes privées n'y sont tenues que si, régulièrement, elles:

- a. Traitent des données sensibles ou des profils de la personnalité, sans y être obligées légalement et à l'insu des personnes concernées; ou
- b. Communiquent des données à des tiers, sans y être obligées légalement et à l'insu des personnes concernées.

³ Les fichiers doivent être déclarés avant d'être opérationnels.

⁴ Le Conseil fédéral règle les modalités de déclaration des fichiers, de même que la tenue et la publication du registre. Il peut prévoir, pour certains types de fichiers, des exceptions à l'obligation de déclarer ou d'enregistrer lorsque, le traitement ne menace pas la personnalité des personnes concernées.

Art. 8 Communication à l'étranger

¹ Celui qui entend communiquer, régulièrement ou en grand nombre, des données personnelles à l'étranger, doit le déclarer préalablement au préposé fédéral à la protection des données si:

- a. La communication ne découle pas d'une obligation légale; ou
- b. Elle a lieu à l'insu des personnes concernées.

² Le Conseil fédéral règle les modalités de la déclaration. Il peut prévoir des déclarations simplifiées ou des exceptions à l'obligation de déclarer lorsque, le traitement ne menace pas la personnalité des personnes concernées.

Section 3:

Traitement de données personnelles par des personnes privées

Art. 9 Atteintes à la personnalité

¹ Celui qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées.

² Il n'est notamment pas en droit, sans motif justificatif, de:

- a. Traiter des données en violation des principes définis à l'article 4;
- b. Traiter des données au mépris de la volonté expresse de la personne concernée;
- c. Communiquer à des tiers des données sensibles ou des profils de la personnalité.

Art. 10 Motifs justificatifs

¹ Une atteinte à la personnalité est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.

² Celui qui traite des données personnelles peut notamment se voir reconnaître un intérêt prépondérant, si:

- a. Le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant;

- b. Le traitement s'inscrit dans un rapport de concurrence économique, actuel ou futur, avec une personne dont la raison est inscrite au registre du commerce, à condition toutefois qu'aucune donnée traitée ne soit communiquée à des tiers;
- c. Les données sont traitées dans le but d'évaluer le crédit d'une personne dont la raison est inscrite au Registre du commerce, à condition toutefois qu'elles ne soient pas sensibles et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée;
- d. Les données sont traitées en vue d'une publication dans un média à caractère périodique;
- e. Les données sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées;
- f. Les données traitées ont été rendues accessibles à tout un chacun par la personne concernée.

Art. 11 Traitement de données par un tiers

¹ Le traitement de données personnelles peut être confié à un tiers, si:

- a. Le mandant veille à ce que ne soient pas effectués des traitements autres que ceux qu'il est lui-même en droit d'effectuer; et
- b. Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

² Le tiers peut faire valoir les mêmes motifs justificatifs que le mandant.

Art. 12 Actions et procédure

¹ Les articles 28 à 28f du code civil¹⁾ régissent les actions et les mesures provisionnelles concernant la protection de la personnalité. Le demandeur peut en particulier requérir la rectification ou la destruction des données personnelles.

² Si ni l'exactitude, ni l'inexactitude des données ne peut être prouvée, la personne concernée peut demander que l'on ajoute aux données la mention de leur caractère litigieux.

³ Les actions en exécution du droit d'accès peuvent être ouvertes au domicile du demandeur ou à celui du défendeur. Le juge statue selon une procédure simple et rapide.

¹⁾ RS 210

Section 4:

Traitement de données personnelles par des organes fédéraux

Art. 13 Organe responsable

¹ Il incombe à l'organe fédéral de pourvoir à la protection des données qu'il traite ou fait traiter dans l'accomplissement de ses tâches.

² Lorsqu'un organe fédéral traite des données conjointement avec d'autres organes fédéraux, avec des organes cantonaux ou avec des personnes privées, le Conseil fédéral peut régler de manière spécifique les responsabilités en matière de protection des données.

Art. 14 Bases juridiques

¹ Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale à cet effet.

² Des données sensibles ou des profils de la personnalité ne peuvent être traités que si:

- a. Une loi au sens formel le prévoit expressément;
- b. L'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument;
- c. Le Conseil fédéral l'a autorisé, considérant que les droits des personnes concernées ne sont pas menacés; ou
- d. La personne concernée y a, en l'espèce, consenti ou a rendu ses données accessibles à tout un chacun.

Art. 15 Collecte de données personnelles

¹ La collecte de données personnelles doit être effectuée de façon reconnaissable pour les personnes concernées.

² L'organe fédéral qui collecte systématiquement des données, notamment au moyen de questionnaires, est tenu de préciser le but et la base juridique du traitement, les catégories de participants au fichier et de destinataires des données.

³ Il n'est pas nécessaire de se conformer à ces exigences si:

- a. La personne concernée a rendu ses données accessibles à tout un chacun;
- b. L'accomplissement de la tâche de l'organe fédéral est compromis; ou
- c. Il en résulte un volume excessif de travail.

Art. 16 Communication de données personnelles

¹ Les organes fédéraux ne sont en droit de communiquer des données personnelles que s'il existe une base juridique au sens de l'article 14 ou si:

- a. Le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale;

- b. La personne concernée y a, en l'espèce, consenti ou les circonstances permettent de présumer un tel consentement;
 - c. La personne concernée a rendu ses données accessibles à tout un chacun; ou si
 - d. Le destinataire rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes; dans la mesure du possible, la personne concernée sera auparavant invitée à se prononcer.
- ² Dans tous les cas, les organes fédéraux sont en droit de communiquer, sur demande, le nom, le prénom, l'adresse et la date de naissance d'une personne.
- ³ L'organe fédéral refuse la communication, la restreint ou l'assortit de charges, si:
- a. Un important intérêt public ou un intérêt légitime manifeste de la personne concernée l'exige; ou si
 - b. Une obligation légale de garder le secret ou une disposition particulière de protection des données l'exige.

Art. 17 Blocage des données

- ¹ La personne concernée qui rend vraisemblable un intérêt légitime peut s'opposer à ce que l'organe fédéral responsable communique des données personnelles déterminées.
- ² L'organe fédéral lève l'opposition si:
- a. Il est juridiquement tenu de communiquer les données; ou si
 - b. Le défaut de communication compromettrait l'accomplissement de ses tâches.

Art. 18 Obligation de rendre les données personnelles anonymes ou de les détruire

Les organes fédéraux sont tenus de rendre anonymes ou de détruire les données personnelles dont ils n'ont plus besoin, à moins qu'elles:

- a. Ne doivent être conservées à titre de preuve ou par mesure de sûreté; ou qu'elles
- b. Ne doivent être déposées aux Archives fédérales.

Art. 19 Traitements aux fins de recherche, de planification et de statistique

- ¹ Les organes fédéraux sont en droit de traiter des données personnelles et de les communiquer à des tiers, à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, si:
- a. Les données sont rendues anonymes dès que le but du traitement le permet;
 - b. Le destinataire ne communique les données qu'avec le consentement de l'organe fédéral; et

c. Les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

² Il n'est pas nécessaire de se conformer aux dispositions suivantes:

- a. L'article 4, 4^e alinéa, relatif au but du traitement;
- b. L'article 14, 2^e alinéa, relatif à la base juridique pour le traitement de données sensibles et de profils de la personnalité; et
- c. L'article 16, 1^{er} alinéa, relatif à la communication de données.

Art. 20 Activités de droit privé des organes fédéraux

¹ Lorsqu'un organe fédéral agit selon le droit privé, le traitement des données est régi par les dispositions applicables aux personnes privées.

² Toutefois, la surveillance s'exerce conformément aux règles applicables aux organes fédéraux.

Art. 21 Protection de l'Etat et sécurité militaire

¹ Lorsque des données personnelles sont traitées par des organes chargés de la protection de l'Etat ou de la sécurité militaire, le Conseil fédéral peut:

- a. Prévoir des exceptions aux dispositions relatives au but du traitement (art. 4, 4^e al.) et à la communication à l'étranger (art. 4, 5^e al.);
- b. Autoriser le traitement de données sensibles ou de profils de la personnalité, même si les conditions posées à l'article 14, 2^e alinéa, et à l'article 16, 1^{er} alinéa, ne sont pas remplies;
- c. Lever les obligations de déclarer et d'enregistrer (art. 7 et 8);
- d. Régler la coopération avec le préposé à la protection des données en dérogation à l'article 24, 3^e alinéa.

² Le secret de vote, le secret de pétition et le secret des statistiques demeurent garanties.

³ Le département dont relève l'organe concerné tranche les différends en lieu et place de la Commission fédérale de la protection des données (art. 27, 2^e al.) ou de son président (art. 25, 2^e al., et 27, 3^e al.). Il prend l'avis du préposé à la protection des données. En lieu et place du Tribunal fédéral les recours sont portés devant le Conseil fédéral.

Art. 22 Prétentions et procédure

¹ Celui qui a un intérêt légitime peut exiger de l'organe fédéral responsable qu'il:

- a. S'abstienne de procéder à un traitement illicite;
- b. Supprime les effets d'un traitement illicite;
- c. Constate le caractère illicite du traitement.

² Il peut en particulier demander que l'organe fédéral:

- a. Rectifie ou détruit les données;
- b. Publie ou communique à des tiers la décision ou la rectification.

³ Si ni l'exactitude, ni l'inexactitude d'une donnée ne peut être prouvée, l'organe fédéral doit ajouter à la donnée la mention de son caractère litigieux.

⁴ La procédure est régie par la loi fédérale sur la procédure administrative¹⁾. Toutefois, les exceptions prévues par les articles 2 et 3 de cette loi ne sont pas applicables.

⁵ Les décisions des organes fédéraux peuvent être portées devant la Commission fédérale de la protection des données.

Section 5: Préposé fédéral à la protection des données

Art. 23 Nomination et statut

¹ Le préposé fédéral à la protection des données est nommé par le Conseil fédéral.

² Il s'acquitte de ses tâches de manière autonome et il est rattaché administrativement au Département fédéral de justice et police.

³ Il dispose d'un secrétariat permanent.

Art. 24 Surveillance

¹ Le préposé surveille l'application de la présente loi et des autres dispositions relatives à la protection des données. Aucune surveillance ne peut être exercée sur le Conseil fédéral.

² Il peut élucider les faits, d'office ou à la demande de tiers, lorsque:

- a. Une personne privée recourt à une méthode de traitement susceptible de porter atteinte à la personnalité d'un nombre important de personnes;
- b. Des fichiers doivent être enregistrés (art. 7);
- c. Des communications à l'étranger doivent être déclarées (art. 8);
- d. Des données sont traitées par des organes fédéraux.

³ Aux fins d'élucider les faits, il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. Les personnes impliquées sont tenues de collaborer à l'établissement des faits. Le droit de refuser le témoignage au sens de l'article 16 de la loi fédérale sur la procédure administrative¹⁾ s'applique par analogie.

⁴ S'il apparaît que des prescriptions sur la protection des données ont été violées, le préposé recommande de modifier ou de cesser le traitement.

⁵ Si une recommandation du préposé est rejetée ou n'est pas suivie, le préposé peut:

- a. Porter l'affaire devant la Commission fédérale de la protection des données qui décide; ou
- b. Informer la personne concernée qui s'est adressée à lui du résultat et lui indiquer les voies de droit (art. 12 et 22).

¹⁾ RS 172.021

Art. 25 Information

¹ Le préposé fait rapport au Conseil fédéral à intervalles réguliers et selon les besoins. Les rapports périodiques sont publiés.

² S'il y va de l'intérêt général, il peut informer le public de ses constatations et de ses recommandations. Il ne peut porter à la connaissance du public des données soumises au secret de fonction qu'avec le consentement de l'autorité compétente. Si celle-ci ne donne pas son consentement, le président de la Commission fédérale de la protection des données tranche; sa décision est définitive.

Art. 26 Autres attributions

¹ Le préposé a notamment les autres attributions suivantes:

- a. Assister les personnes privées ainsi que les organes fédéraux et cantonaux en les informant, en les conseillant et en leur servant d'intermédiaire;
- b. Se prononcer sur les projets d'actes législatifs fédéraux et de mesures fédérales qui ont de l'importance pour la protection des données;
- c. Collaborer avec les autorités chargées de la protection des données en Suisse et à l'étranger;
- d. Apprécier dans quelle mesure la protection des données assurée à l'étranger est comparable à celle que connaît la Suisse.

² Le préposé peut donner aux organes de l'administration fédérale des conseils en matière de protection des données, même si la présente loi n'est pas applicable en vertu de l'article 2, 2^e alinéa, lettres e à h. Les organes peuvent lui accorder l'accès à leurs dossiers.

³ Le préposé conseille la Commission d'experts du secret professionnel en matière de recherche médicale (art. 321^{bis} CP¹⁾). Si cette commission a autorisé la levée du secret professionnel, il surveille le respect des charges qui grèvent l'autorisation. A cet effet il peut élucider les faits au sens de l'article 24, 3^e alinéa. Il peut porter les décisions de la commission d'experts devant la Commission fédérale de la protection des données.

Section 6: Commission fédérale de la protection des données

Art. 27

¹ La Commission fédérale de la protection des données est une commission d'arbitrage et de recours au sens des articles 71a à 71c, lettres a à c, de la loi fédérale sur la procédure administrative²⁾.

² Elle statue sur:

- a. Les recommandations du préposé (art. 24, 5^e al.) qui lui ont été soumises;
- b. Les recours contre les décisions des organes fédéraux en matière de protection des données à l'exception de celles du Conseil fédéral;

¹⁾ RS 311.0

²⁾ RS 172.021

- c. Les recours contre les décisions de la Commission du secret professionnel en matière de recherche médicale (art. 321^{bis} CP¹⁾);
- d. Les recours contre les décisions cantonales de dernière instance prises en application de dispositions de droit public fédéral relatives à la protection des données.

³ Le préposé peut requérir des mesures provisionnelles du président de la commission, s'il constate, à l'issue de l'enquête qu'il a menée en application de l'article 24, 2^e alinéa, que la personne concernée risque de subir un préjudice difficilement réparable. Les articles 79 à 84 de la loi fédérale sur la procédure civile fédérale²⁾ s'appliquent par analogie à la procédure.

Section 7: Dispositions pénales

Art. 28 Violation des obligations de renseigner, de déclarer et de collaborer

¹ Les personnes privées qui, intentionnellement, auront donné de manière inexacte ou incomplète un renseignement qu'elles sont tenues de fournir selon les articles 5 et 6 seront, sur plainte, punies des arrêts ou de l'amende.

² Seront punies des arrêts ou de l'amende, les personnes privées qui, intentionnellement:

- a. N'auront pas déclaré un fichier conformément à l'article 7 ou une communication à l'étranger conformément à l'article 8, ou auront donné des indications inexactes lors de la déclaration;
- b. Auront fourni au préposé à la protection des données, lors de l'élucidation des faits (art. 24, 3^e al.), des renseignements inexacts ou auront refusé leur collaboration.

Art. 29 Violation du devoir de discrétion

¹ Celui qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles dont il a eu connaissance dans l'exercice d'une profession qui requiert la connaissance de telles données, sera, sur plainte, puni des arrêts ou de l'amende.

² Est passible de la même peine celui qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles, dont il a eu connaissance dans le cadre des activités qu'il exerce pour le compte de la personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle.

³ La révélation illicite de données personnelles secrètes et sensibles demeure punissable alors même que les rapports de travail ou de formation ont pris fin.

¹⁾ RS 311.0

²⁾ RS 273

Section 8: Dispositions finales

Art. 30 Exécution

¹ Le Conseil fédéral édicte les dispositions d'exécution.

² Il règle le traitement des données qui sont déposées aux Archives fédérales. A cet effet, il peut prévoir des dérogations aux articles 5 et 6 régissant le droit d'accès ainsi qu'aux articles 14, 2^e alinéa, et 16, 1^{er} alinéa, relatifs au traitement de données sensibles.

³ Il peut prévoir des dérogations aux articles 5 et 6 en ce qui concerne l'octroi de renseignements par les représentations diplomatiques et consulaires suisses à l'étranger.

⁴ Il peut en outre déterminer:

- a. Les fichiers dont le traitement doit faire l'objet d'un règlement;
- b. Les conditions auxquelles un organe fédéral peut faire traiter des données personnelles par un tiers ou les traiter pour le compte d'un tiers;
- c. Le mode selon lequel les moyens d'identification de personnes peuvent être utilisés.

⁵ Il peut conclure des traités internationaux en matière de protection des données, dans la mesure où ils sont conformes aux principes établis par la présente loi.

⁶ Il règle la manière de mettre en sûreté les fichiers dont les données, en cas de guerre ou de crise, sont de nature à mettre en danger la vie ou l'intégrité corporelle des personnes concernées.

Art. 31 Dispositions transitoires

¹ Au plus tard une année après l'entrée en vigueur de la présente loi, les maîtres de fichier doivent déclarer les fichiers existants en vue de l'enregistrement prévu à l'article 7.

² Dans le délai d'une année à compter de l'entrée en vigueur de la présente loi, ils doivent prendre les mesures nécessaires à assurer l'exercice du droit d'accès au sens de l'article 5.

³ Les organes fédéraux peuvent continuer à utiliser pendant cinq ans, à compter de l'entrée en vigueur de la présente loi, les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité, quand bien même les conditions de traitement posées à l'article 14, 2^e alinéa, ne sont pas réunies.

Art. 32 Référendum et entrée en vigueur

¹ La présente loi est sujette au référendum facultatif.

² Le Conseil fédéral fixe la date de l'entrée en vigueur.

Modification de lois fédérales

1. Le code des obligations¹⁾ est modifié comme il suit:

Art. 328b (nouveau)

3. Lors du traitement de données personnelles

¹ L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail.

² Il ne peut donner à des tiers des renseignements sur le travailleur que si une disposition légale l'y autorise ou si le travailleur y a consenti.

³ Dans la mesure où les articles 5 et 6 de la loi fédérale du . . . ²⁾ sur la protection des données lui confèrent un droit d'accès, le travailleur qui le demande doit être autorisé par l'employeur à consulter les données le concernant.

Art. 362

...

Article 328b (Protection de la personnalité lors du traitement de données personnelles)

...

2. La loi fédérale du 18 décembre 1987³⁾ sur le droit international privé (LDIP) est modifiée comme il suit:

Art. 130, 3^e al. (nouveau)

³ Les actions en exécution du droit d'accès dirigées contre le maître du fichier peuvent être intentées devant les tribunaux mentionnés à l'article 129 ou devant les tribunaux suisses du lieu où le fichier est géré ou utilisé.

Art. 139, 3^e al. (nouveau)

³ Le 1^{er} alinéa s'applique également aux atteintes à la personnalité résultant du traitement de données personnelles ainsi qu'aux entraves mises à l'exercice du droit d'accès aux données personnelles.

¹⁾ RS 220

²⁾ RO ...

³⁾ FF 1988 I 5; RO ...

3. Le code pénal suisse¹⁾ est modifié comme il suit:

Art. 179^{novies} (nouveau)

Soustraction de
données
personnelles

Celui qui aura soustrait d'un fichier des données personnelles sensibles qui ne sont pas librement accessibles, sera, sur plainte, puni de l'emprisonnement ou de l'amende.

Art. 321^{bis} (nouveau)

Secret
professionnel
en matière de
recherche
médicale

¹ Un secret professionnel peut être levé à des fins de recherche dans les domaines de la médecine ou de la santé publique si une commission d'experts en donne l'autorisation et si l'intéressé n'a pas expressément refusé son consentement.

² La commission octroie l'autorisation, si:

- a. La recherche ne peut être effectuée avec des données anonymes;
- b. Il est impossible ou particulièrement difficile d'obtenir le consentement de l'intéressé; et si
- c. Les intérêts de la recherche priment l'intérêt au maintien du secret.

³ La commission grève l'autorisation de charges afin de garantir la protection des données. Elle publie l'autorisation.

⁴ La commission peut octroyer des autorisations générales ou prévoir d'autres simplifications si aucun intérêt légitime des intéressés n'est compromis et si les données personnelles sont rendues anonymes dès le début des recherches. Le Conseil fédéral règle les modalités.

⁵ Le Conseil fédéral nomme la commission. Il en règle l'organisation et la procédure. La commission agit sans instructions.

⁶ Celui qui aura révélé un secret dont il avait eu connaissance à raison de ses activités de recherche menées dans les domaines de la médecine et de la santé publique, sera puni en conformité de l'article 321.

4. La loi fédérale sur la procédure pénale²⁾ est modifiée comme il suit:

IV. Entraide judiciaire (nouveau)

Art. 26^{bis}

¹ Les autorités de la Confédération, des cantons et des communes assistent dans l'accomplissement de leur tâche les autorités chargées de poursuivre et de juger

¹⁾ RS 311.0

²⁾ RS 312.0

les affaires de droit pénal fédéral; elles doivent en particulier leur donner les renseignements dont elles ont besoin et leur permettre de consulter les pièces officielles qui peuvent avoir de l'importance pour la poursuite pénale.

- ² L'entraide judiciaire peut être refusée, restreinte ou assortie de charges, si
- a. Des intérêts publics importants ou des intérêts manifestement légitimes d'une personne concernée l'exigent; ou
 - b. Le secret professionnel (art. 77) s'y oppose.

³ Les organisations chargées de tâches de droit public sont, dans les limites de ces tâches, tenues de prêter assistance de la même manière que les autorités.

⁴ Les contestations entre autorités administratives fédérales sont tranchées par le Département dont relèvent les autorités concernées ou par le Conseil fédéral, les contestations entre Confédération et cantons le sont par la Chambre d'accusation du Tribunal fédéral.

⁵ Au surplus, sont applicables en matière d'entraide judiciaire les articles 352 ss du code pénal suisse¹⁾, de même que l'article 18 de la loi fédérale d'organisation judiciaire²⁾.

Art. 52, 2^e alinéa, deuxième phrase

Abrogée

IX. Du traitement de données personnelles, du séquestre, de la perquisition, de la confiscation et de la surveillance (nouveau)

Art. 64^{bis} (nouveau)

¹ Toute donnée personnelle doit également être collectée de façon reconnaissable auprès de la personne concernée, à moins que l'instruction n'en soit compromise ou qu'il n'en résulte un volume excessif de travail.

² Si une donnée personnelle est rectifiée ou détruite, ou si son exactitude n'a pu être prouvée (art. 102^{bis}, 3^e et 4^e al.), les organes compétents en avertissent sans délai toute autorité ou organe à qui la donnée a été communiquée.

³ Les données personnelles qui ne sont plus nécessaires à la conduite de l'instruction doivent être détruites au plus tard à sa clôture. Toutefois, elles peuvent être utilisées dans le cadre d'une autre procédure dans la mesure où celle-ci l'exige.

Titre précédant l'article 65

Abrogé

Art. 72^{bis} (nouveau)

La police peut photographier ou filmer les participants à une manifestation se déroulant dans la légalité s'il ressort des circonstances concrètes que certaines de

¹⁾ RS 311.0

²⁾ RS 173.110

ces personnes envisagent de commettre un crime ou un délit dont la gravité ou la particularité justifie cette mesure.

IX^{bis}. De la fouille, de l'examen médical et des mesures d'identification (nouveau)

Art. 73^{bis} (nouveau)

¹ La police judiciaire peut fouiller une personne si:

- a. Les conditions permettant de l'appréhender sont réunies;
- b. Celle-ci est soupçonnée de détenir des objets qui doivent être mis en sûreté;
- c. Celle-ci ne peut être identifiée autrement; ou
- d. Celle-ci se trouve manifestement dans un état l'empêchant de se déterminer librement et si la fouille est indispensable à sa protection.

² La police judiciaire peut fouiller une personne afin de rechercher des armes, des outils dangereux ou des explosifs si, au vu des circonstances, la sécurité des agents de police ou de tiers l'exige.

³ Sauf cas d'urgence, seule une personne du même sexe ou un médecin peut procéder à la fouille.

Art. 73^{ter} (nouveau)

¹ Si nécessaire, le juge peut ordonner l'examen physique ou psychique de l'inculpé afin:

- a. D'établir les faits; ou
- b. De déterminer sa capacité de discernement, son aptitude à participer aux débats ou à supporter une détention, ou encore la nécessité d'ordonner une mesure à son encontre.

² Tant que l'instruction préparatoire n'a pas été ouverte, il appartient au procureur général d'ordonner l'examen physique ou psychique.

³ Une personne non inculpée ne peut être examinée sans son consentement que s'il s'agit d'élucider un fait qui ne peut l'être par un autre moyen. Aucune personne en droit de refuser de témoigner ne peut être contrainte à subir un examen physique ou psychique.

⁴ L'examen doit être confié à un médecin ou à une autre personne qualifiée. Une atteinte à l'intégrité corporelle n'est licite que si tout risque de préjudice est écarté.

⁵ En cas de forts soupçons, la police judiciaire peut ordonner une prise de sang.

Art. 73^{quater} (nouveau)

La police judiciaire peut soumettre à des mesures d'identification:

- a. Un inculpé, si l'administration des preuves l'exige;
- b. D'autres personnes aux fins de déterminer l'origine de traces.

Art. 101^{bis} (nouveau)

La police judiciaire peut requérir des informations orales ou écrites ou entendre des personnes à titre de renseignement; celui qui est en droit de refuser son témoignage doit être préalablement avisé qu'il n'est pas obligé de répondre.

Art. 102^{bis} (nouveau)

¹ Toute personne peut demander au Ministère public de la Confédération, quelles données la concernant sont traitées par la police judiciaire.

² Le procureur général peut refuser de donner les renseignements demandés si:

- a. Leur octroi compromettrait les recherches;
- b. Des intérêts publics prépondérants, en particulier la sûreté intérieure ou extérieure de la Confédération, l'exigent; ou
- c. Des intérêts prépondérants de tiers l'exigent.

³ Celui qui a un intérêt légitime peut exiger de la police judiciaire qu'elle rectifie des données inexactes ou qu'elle les détruise.

⁴ La preuve de l'exactitude d'une donnée doit être apportée par la police judiciaire. Si ni l'exactitude, ni l'inexactitude ne peut être prouvée, mention en est faite au dossier.

Art. 102^{ter} (nouveau)

¹ Si le procureur général ne fait pas droit à une demande de renseignements, de rectification ou de destruction, le requérant peut demander au préposé fédéral à la protection des données de contrôler le bien-fondé de la décision négative.

² Le préposé adresse au procureur général une recommandation, déclarant dans quelle mesure il convient de communiquer au requérant les renseignements demandés ou s'il convient de donner suite à la demande de rectification ou de destruction.

³ Si le procureur général et le préposé ne parviennent pas à se mettre d'accord, ils peuvent porter l'affaire devant la Chambre d'accusation du Tribunal fédéral.

Art. 102^{quater} (nouveau)

¹ Tant que l'instruction préparatoire n'a pas été ouverte, les données afférentes aux recherches de la police judiciaire ne peuvent être communiquées qu'aux seuls organes suivants:

- a. Au Conseil fédéral;
- b. Aux organes de police judiciaire et aux autorités judiciaires fédérales et cantonales, s'ils en ont besoin dans le cadre d'une procédure;
- c. Aux organes chargés de la protection de l'Etat et de la sécurité militaire;
- d. Aux organes de police judiciaire d'Etats étrangers ou à d'autres organes administratifs étrangers chargés de tâches de police, dans les limites de l'article 16 de la loi fédérale du ...¹⁾ sur la protection des données;

¹⁾ RO ...

- e. Au préposé fédéral à la protection des données;
- f. A l'Office fédéral de la police, dans la mesure où celui-ci a besoin des données pour accomplir les tâches que lui attribuent les lois fédérales sur l'entraide judiciaire internationale en matière pénale ou dans la mesure où les données doivent être enregistrées dans le système de recherches informatisées RIPOL;
- g. Au Département fédéral de justice et police, lorsqu'il doit donner l'autorisation d'ouvrir une poursuite pénale contre un fonctionnaire, ainsi qu'à l'autorité dont relève le fonctionnaire afin qu'elle puisse se déterminer sur l'autorisation.

² Les autres dispositions en matière d'entraide judiciaire sont réservées.

Art. 105^{bis} (nouveau)

¹ Les mesures de contrainte ordonnées ou confirmées par le procureur général sont sujettes à recours devant la Chambre d'accusation du Tribunal fédéral dans les dix jours.

² Les articles 215 à 219 régissent, par analogie, les recours contre les ordres de détention.

Art. 107^{bis} (nouveau)

¹ Au terme de la procédure fédérale ou cantonale, le Ministère public de la Confédération détruit les pièces ou les archive. Sont réservées celles qui doivent être versées aux Archives fédérales.

² Les pièces archivées au Ministère public ou aux Archives fédérales peuvent être utilisées dans le cadre d'une autre procédure et pour des traitements ne se rapportant pas à des personnes.

³ Le Conseil fédéral règle les modalités.

- 5. La loi fédérale du 20 mars 1981¹⁾ sur l'entraide internationale en matière pénale (loi sur l'entraide pénale internationale [EIMP]) est modifiée comme il suit:

Section 2^{bis}: Collaboration avec INTERPOL (nouveau)

Art. 81a Compétence

¹ Le Ministère public de la Confédération fonctionne comme Bureau central national au sens des statuts de l'Organisation internationale de police criminelle (INTERPOL).

² Il lui appartient de procéder à des échanges d'informations entre les autorités fédérales et cantonales de poursuite pénale, d'une part, et les bureaux centraux nationaux d'autres Etats et le Secrétariat général d'INTERPOL d'autre part.

¹⁾ RS 351.1

Art. 81b Attributions

¹ Le Ministère public de la Confédération transmet des informations de police criminelle aux fins de poursuivre des infractions ou d'assurer l'exécution de peines et de mesures.

² Il peut transmettre des informations de police criminelle aux fins de prévenir des infractions si, au vu des circonstances réelles, la commission d'un crime ou d'un délit est très probable.

³ Il peut transmettre des informations destinées à rechercher des personnes disparues ou à identifier des inconnus.

⁴ En vue de prévenir ou d'élucider des infractions, le Ministère public de la Confédération peut recevoir des informations provenant de particuliers ou donner des informations à des particuliers, si cela est dans l'intérêt des personnes concernées et si celles-ci ont donné leur accord ou si les circonstances permettent de le présumer.

Art. 81c Protection des données

¹ Les échanges d'informations de police criminelle s'effectuent conformément aux principes de la présente loi ainsi qu'aux statuts et aux règlements d'INTERPOL que le Conseil fédéral aura déclarés applicables.

² La loi fédérale du ...¹⁾ sur la protection des données régit les échanges d'informations opérés en vue de rechercher des personnes disparues et d'identifier des inconnus, ainsi qu'à des fins administratives.

³ Le Ministère public de la Confédération peut transmettre des informations directement aux bureaux centraux nationaux d'autres pays, si l'Etat destinataire est soumis aux prescriptions d'INTERPOL en matière de protection des données.

Art. 81d Aides financières et indemnités

La Confédération peut octroyer à INTERPOL des aides financières et des indemnités.

32077

¹⁾ RO ...

Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988

In	Bundesblatt
Dans	Feuille fédérale
In	Foglio federale
Jahr	1988
Année	
Anno	
Band	2
Volume	
Volume	
Heft	18
Cahier	
Numero	
Geschäftsnummer	88.032
Numéro d'affaire	
Numero dell'oggetto	
Datum	10.05.1988
Date	
Data	
Seite	421-539
Page	
Pagina	
Ref. No	10 105 439

Das Dokument wurde durch das Schweizerische Bundesarchiv digitalisiert.
Le document a été digitalisé par les. Archives Fédérales Suisses.
Il documento è stato digitalizzato dell'Archivio federale svizzero.