03.016

Message

relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données

du 19 février 2003

Messieurs les Présidents,
Mesdames et Messieurs,

Par le présent message, nous soumettons à votre approbation le projet de révision de la loi fédérale sur la protection des données du 19 juin 1992 et l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données.

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

2000	M	00.3000	Renforcement de la transparence lors de la collecte de données personnelles (E 28.01.2000, Commission des affaires juridiques CE)
1999	M	98.3529	Liaisons «online». Renforcer la protection pour les données personnelles (E 17.11.1998, Commission de gestion CE)

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

19 février 2003 — Au nom du Conseil fédéral suisse:

Le président de la Confédération, Pascal Couchepin
La chancelière de la Confédération, Annemarie Huber-Hotz

Condensé

La présente révision vise principalement l'amélioration de l'information des personnes sur lesquelles des données sont collectées, la fixation d'un niveau de protection minimum lorsque les autorités cantonales traitent des données en exécution du droit fédéral et la transposition dans le droit suisse des principes prévus par le Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données.

Contexte et but du projet de révision

La présente révision a pour origine deux motions adoptées en 1999 et 2000 par les Chambres fédérales, qui demandaient d'une part davantage de transparence lors de la collecte de données et d'autre part une base légale formelle pour tout accès en ligne à des données traitées par des organes fédéraux ainsi qu'un standard minimum de protection lorsque des données sont traitées par les cantons en exécution du droit fédéral. En outre, certaines dispositions de la loi fédérale sur la protection des données doivent être modifiées pour permettre l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données.

L'expérience faite en matière de protection des données a démontré que l'application de la loi fédérale sur la protection des données est de manière générale satisfaisante, même si cette loi présente quelques défauts ponctuels, notamment par rapport aux moyens accordés aux personnes concernées pour s'opposer au traitement de données les concernant.

Contenu du projet de révision

Le projet de révision prévoit l'obligation pour les personnes privées et les organes fédéraux d'informer activement la personne concernée lorsqu'ils collectent des données sensibles et des profils de la personnalité à son sujet. La personne concernée doit au moins être informée de l'identité du maître du fichier, des finalités du traitement pour lequel les données sont collectées et des catégories de destinataires des données si la communication est envisagée. Pour les données personnelles qui ne sont pas des données sensibles ni des profils de la personnalité, la collecte doit au moins être reconnaissable pour la personne concernée.

Le projet de révision assortit en outre l'obligation de déclarer les fichiers d'un certain nombre d'exceptions et renforce la position des personnes qui s'opposent à un traitement de données les concernant. Il fixe également des exigences minimales auxquelles les cantons doivent satisfaire en matière de protection des données quand ils exécutent le droit fédéral et renforce les possibilités de contrôle sur ceux-ci lorsqu'ils traitent des données personnelles en application du droit fédéral.

Le projet de révision permet au Conseil fédéral d'autoriser, pour une durée limitée, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre de projets pilotes, avant qu'une loi au sens formel ne soit entrée en vigueur.

Enfin, pour rendre la législation suisse conforme au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données, le projet de révision harmonise les conditions auxquelles est subordonnée la communication transfrontière de données avec le droit européen et accorde la qualité pour recourir au Préposé fédéral à la protection des données dans le cadre de la surveillance des organes fédéraux.

Message

1 Partie générale

1.1 Contexte

1.1.1 Droit en vigueur

1.1.1.1 Au niveau fédéral

La protection des données est actuellement régie, au niveau fédéral, par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[1], loi entrée en vigueur le 1er juillet 1993 et qui régit le traitement de données concernant des personnes physiques et morales effectué par des personnes privées et des organes fédéraux (art. 2).

La LPD fixe les principes à respecter lors du traitement de données personnelles. Elle prescrit en particulier que toute collecte de données personnelles ne peut être entreprise que d'une manière licite (art. 4, al. 1), que leur traitement doit être effectué conformément aux principes de la bonne foi et de la proportionnalité (art. 4, al. 2) et que les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de la collecte, qui est prévu par une loi ou qui ressort des circonstances (art. 4, al. 3). La personne ou l'organe qui traite des données personnelles doit en outre s'assurer qu'elles sont correctes (art. 5).

La LPD règle la communication des données à l'étranger (art. 6), de même que le droit d'accès (art. 8). Elle interdit aux personnes privées qui traitent des données personnelles de porter une atteinte illicite à la personnalité des personnes concernées (art. 12, al. 1,) et en particulier de traiter des données contre la volonté expresse de la personne concernée en l'absence de motif justificatif (art. 12, al. 2, let. b). Elle règle les prétentions que les personnes lésées peuvent faire valoir, ainsi que la procédure (art. 15).

Les art. 16 à 25 LPD régissent le traitement de données personnelles par des organes fédéraux. Les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale (art. 17, al. 1). Une base légale formelle est exigée pour le traitement de données sensibles ou de profils de la personnalité (art. 17, al. 2). La communication de données personnelles à des tiers est en outre subordonnée à l'existence d'une base juridique, sous réserve des exceptions prévues par la loi (art. 19, al. 1). Les données personnelles ne peuvent être rendues accessibles au moyen d'une procédure d'appel que si cela est prévu expressément (art. 19, al. 3). Les exigences sont encore plus strictes pour les données sensibles ou les profils de la personnalité, lesquels ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément (art. 19, al. 3).

La LPD règle aux art. 26 à 32 les tâches et les compétences du Préposé fédéral à la protection des données (ci-après «Préposé»). Celui-ci surveille l'application de la loi par les organes fédéraux et conseille les personnes privées. Il a la compétence d'effectuer des enquêtes et peut émettre des recommandations. Lorsqu'une recommandation n'est pas suivie dans le secteur privé, il peut porter l'affaire devant la Commission fédérale de la protection des données (art. 28, al. 4). Dans le secteur

[1] RS **235.1**

public, il peut porter l'affaire pour décision auprès du département ou de la Chancellerie fédérale (art. 27, al. 5). Le Préposé n'a pas qualité pour recourir lui-même contre les décisions rendues par les départements et la Chancellerie fédérale[2].

1.1.1.2 Au niveau cantonal

Le traitement de données personnelles par les autorités cantonales est en principe régi par le droit cantonal (art. 2, al. 1, LPD), que ces données aient été obtenues directement par elles ou qu'elles les aient reçues par un accès en ligne à une banque de données fédérale. Diverses dispositions du droit fédéral restreignent toutefois l'autonomie cantonale en matière de protection des données[3]. De plus, en vertu de l'art. 37, al. 1, LPD, le traitement de données personnelles par des organes cantonaux en exécution du droit fédéral est régi par certaines dispositions de la LPD, à moins qu'il ne soit soumis à des dispositions cantonales de protection des données. La plupart des cantons ont adopté une loi au sens formel, mais d'autres se fondent sur une ordonnance ou des directives qui ne sont pas toujours publiées.

L'art. 37, al. 2, LPD oblige en outre les cantons à désigner un organe chargé de veiller au respect de la protection des données. Ceux-ci ont procédé à cette désignation de manière différente. Le statut, les pouvoirs et les moyens à disposition de l'organe de contrôle peuvent varier fortement d'un canton à l'autre.

1.1.2 Interventions parlementaires à l'origine de la révision

1.1.2.1 Motion «liaisons online»

La révision partielle de la LPD a été rendue nécessaire par l'adoption d'une motion de la Commission de gestion du Conseil des Etats le 21 décembre 1999 (motion 98.3529 du 17 novembre 1998. Liaisons «online». Renforcer la protection pour les données personnelles; ci-après: motion «Liaisons online»). Cette motion invite le Conseil fédéral à soumettre aux Chambres fédérales une révision de la LPD dans le but d'imposer des bases légales pour toute liaison «online», même s'il s'agit d'un projet pilote, et de prévoir, pour les requêtes et l'installation de liaisons «online» avec les systèmes informatiques de la Confédération, des normes minimales permettant d'améliorer la collaboration entre la Confédération et les cantons.

Le Conseil fédéral a proposé dans sa réponse de transformer la motion en postulat. Concernant le premier point de la motion, il a rappelé qu'en droit actuel une base légale expresse est déjà nécessaire pour établir une procédure d'appel permettant d'accéder en ligne à une banque de données gérée par un organe fédéral (art. 19, al. 3, 1re phrase, LPD). Une base légale expresse dans une loi au sens formel est de plus requise lorsque la procédure d'appel rend accessibles des données sensibles ou des profils de la personnalité (art. 19, al. 3, 2e phrase, LPD). Pour le Conseil fédéral, cette exigence s'applique également durant la phase pilote et il n'est donc pas néces-

2 ATF **123** II 542
3 Cf. art. 16, al. 2, et 37, al. 1, LPD; art. 16, al. 3, LMSI (RS **120**); art. 16, al. 1, et 17, al. 1, LSF (RS **431.01**).

saire de réviser la loi sur ce point. En revanche, il s'est déclaré disposé à proposer une révision de la LPD en vue d'y introduire une réglementation particulière pour la phase pilote d'un projet lorsqu'un motif d'intérêt public important rend indispensable le traitement de données sensibles ou de profils de la personnalité avant l'entrée en vigueur d'une base légale formelle. En effet, lorsque les liaisons projetées n'ont pu être testées en grandeur réelle, il est difficile de circonscrire avec précision le cercle des instances administratives fédérales et cantonales, voire, dans certains cas des personnes privées, pour lesquelles un accès peut être nécessaire. Le fait de pouvoir tester, durant une phase pilote, les accès à des banques de données, en particulier lors de liaisons «online», permettrait de mieux délimiter les besoins d'accès lors de l'élaboration de la base légale formelle.

Sur le second point de la motion, le Conseil fédéral s'est déclaré prêt à fixer au niveau fédéral un standard à respecter en matière d'accès, d'utilisation, de protection et de contrôle des banques de données fédérales. Il a laissé ouverte la question de savoir si la fixation de ce standard devait passer par l'adoption de normes fédérales directement applicables aux cantons ou prendre la forme de normes supplétives qui s'appliqueraient en l'absence d'une réglementation cantonale correspondante.

Lors de l'adoption de la motion par les Chambres, le représentant du Conseil fédéral avait fait savoir qu'il pouvait se rallier à la motion si une marge de manœuvre suffisante était laissée au gouvernement pour réaliser celle-ci dans le sens de sa réponse[4].

1.1.2.2 Motion sur le renforcement de la transparence

Une seconde motion invitant le Conseil fédéral à proposer aux Chambres fédérales une révision de la LPD a été adoptée par les Chambres fédérales le 5 octobre 2000. Il s'agit d'une motion de la Commission des affaires juridiques du Conseil des Etats (motion 00.3000 du 28 janvier 2000. Renforcement de la transparence lors de la collecte des données personnelles; ci-après: motion «Renforcement de la transparence»). Elle demande l'introduction dans la LPD d'une obligation pour les personnes privées et les organes fédéraux d'informer les personnes concernées lors de la collecte de données personnelles sensibles et de profils de la personnalité. Elle prévoit que l'information portera en particulier sur l'identité du maître du fichier, sur les finalités du traitement et sur toutes les informations supplémentaires nécessaires à assurer un traitement des données conforme aux principes de la bonne foi et de la proportionnalité. L'obligation d'informer devra couvrir aussi bien la collecte auprès de la personne concernée que la collecte auprès de tiers. Des exceptions pourront être prévues pour préserver un intérêt public ou privé prépondérant.

1.2 Portée et objectifs de la révision

A la suite de l'adoption des deux motions, un premier projet de révision a été élaboré par l'administration fédérale, sous l'égide de l'Office fédéral de la justice, en collaboration avec le Préposé. La question était de savoir s'il fallait limiter la révision aux domaines visés par les deux motions adoptées par les Chambres fédérales

4 BO **1999** E 212 et N 2599.

ou au contraire l'étendre à d'autres points, voire entamer une révision totale. On pouvait notamment se demander si l'occasion ne devait pas être saisie de rendre la LPD compatible avec le droit communautaire, en particulier avec la Directive 95/46/CE.

Pour recueillir quelques avis, l'Office fédéral de la justice a réuni un groupe de travail informel composé de spécialistes de la protection des données du secteur public et du secteur privé[5], auxquels il a soumis son avant-projet. Les avis exprimés par la plupart d'entre eux ont montré que la LPD avait, dans l'ensemble, fait ses preuves, et qu'une révision totale de la loi serait prématurée à ce stade. La loi présente certes quelques défauts ponctuels auxquels il est possible de remédier dans le cadre d'une révision partielle, mais il serait faux de toucher aux principes matériels de la protection des données. La révision doit donc se limiter à des points pour lesquels le besoin de révision est clairement démontrable ou découle de la réalisation des deux motions mentionnées ci-dessus. Les règles matérielles ne devraient pas être remises en question, mais une amélioration des instruments permettant aux personnes lésées de faire valoir plus efficacement leurs droits peut être envisagée, en complément du renforcement de la transparence demandé par la motion. Le Préposé aurait souhaité quant à lui une révision plus ambitieuse qui, sans remettre en cause les principes fondamentaux de la loi, aurait permis notamment d'harmoniser la législation suisse avec le droit communautaire et de renforcer ses compétences d'investigation, de conseil et de médiation. Dans le cadre des Bilatérales II (en matière de libéralisation des services ainsi que par rapport aux Accords de Schengen et de Dublin), une révision totale sera inévitable à moyen terme si la Suisse s'engage à reprendre les directives communautaires en matière de protection des données. Actuellement, il n'est en revanche pas impératif d'aller au delà de la révision partielle (voir ch. 1.2.3.2). Au besoin, le Conseil fédéral soumettra un message complémentaire au Parlement.

La révision partielle doit en outre permettre à la Suisse de rendre sa législation compatible avec le Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données[6] (ci-après: Protocole additionnel à la Convention STE n° 108). Sur la base des résultats positifs de la consultation, le Conseil fédéral a signé le Protocole additionnel le 17 octobre 2002, sous réserve de son approbation par le Parlement et de sa ratification (voir ch. 1.2.3.1.2).

5 Ces spécialistes sont:
- M. Rainer J. Schweizer, professeur à l'Université de Saint-Gall, président de la Commission fédérale de la protection des données;
- M. Urs Belser, Fürsprecher, Berne;
- Mme Ursula Uttinger, présidente du Datenschutzforum Schweiz;
- M. Markus Siegenthaler, Fürsprecher, Bureau pour la surveillance de la protection des données du canton de Berne;
- M. Gérald Page, avocat et chargé de cours à l'Université, Genève.

6 RS **0.235.1**

1.2.1 Grandes lignes de la révision

Les travaux de révision permettent de renforcer la protection de la personnalité, sans toutefois compliquer inutilement les activités du maître du fichier. S'il est vrai que l'introduction de l'obligation d'informer implique des exigences supplémentaires pour les personnes privées, cette nouvelle obligation est du moins en partie compensé par des allégements. En particulier, la transparence créée par le projet permet de simplifier l'obligation d'enregistrer les fichiers visée à l'art. 11*a*. En outre, l'obligation de déclarer les communications de données à l'étranger (art. 6 LPD) est supprimée et remplacée par une simple obligation ponctuelle d'informer, qui vaut tant pour les personnes privées que pour les organes fédéraux.

Le projet ne déroge pas du principe qui a prévalu jusqu'ici et qui laisse principalement à la personne concernée l'initiative de défendre ses droits. Le Préposé en tant qu'organe de contrôle garde la compétence d'intervenir d'office en établissant les faits et en émettant des recommandations; ses compétences ne sont élargies que de manière limitée.

On part de l'idée que si la personne concernée est informée de la collecte, elle pourra exercer les droits que lui reconnaît la loi et qu'on pourra faire l'économie de mesures plus contraignantes au niveau du contrôle effectué par le Préposé. Cette conception a l'avantage de réduire autant que possible les contraintes à l'égard des personnes qui collectent des données, particulièrement lorsqu'il s'agit de personnes privées, et de laisser dans une large mesure aux personnes concernées le soin de délimiter elles-mêmes jusqu'à quel point elles entendent tolérer d'éventuelles atteintes à leur vie privée. Le but est également de limiter l'information à ce qui est nécessaire et de ne pas inonder les personnes concernées de renseignements qu'elles n'ont pas sollicités, ce qui pourrait être ressenti comme une autre forme d'intrusion, particulièrement lors de transactions courantes.

Le maître du fichier doit également être responsabilisé. C'est pourquoi le projet de révision tend à encourager les mécanismes d'auto-réglementation, à savoir le recours à des procédures de certification et l'octroi de labels de qualité par des organismes indépendants.

Le projet s'efforce en outre de mieux délimiter les responsabilités et le contrôle lorsque le traitement est délégué à des tiers ou confié à des sous-traitants. Il impose au maître du fichier une obligation de diligence, tout en lui laissant, dans plusieurs domaines, une importante marge de manœuvre quant aux moyens de remplir cette obligation. Ainsi, lors de communications transfrontières de données, le maître du fichier doit s'assurer que le destinataire offre un niveau de protection adéquat, mais le projet ne prescrit pas de quelle manière il obtient de telles assurances: celles-ci peuvent découler notamment d'obligations légales, de conventions internationales ou de clauses contractuelles. Le maître du fichier est également libre de choisir la manière dont il entend rendre une collecte de données reconnaissable. Il assume toutefois la responsabilité d'un éventuel préjudice causé par cette collecte.

Le projet donne la faculté au Conseil fédéral d'autoriser pendant un temps limité et à certaines conditions le traitement de données sensibles ou de profils de la personnalité, avant qu'une loi au sens formel ne soit entrée en vigueur.

Enfin, il renforce les exigences et les possibilités de contrôle lors du traitement de données fédérales par des organes cantonaux en exécution du droit fédéral. Dans la mesure où des données fédérales sont traitées, la Confédération dispose d'une base constitutionnelle suffisante pour imposer aux cantons des garanties minimales (cf. ch. 5.1).

En complément de l'obligation d'informer, il est proposé de renforcer les droits des personnes qui entendent s'opposer au traitement de données les concernant. L'expérience montre en effet que la personne qui subit une atteinte peut se trouver dans une position de faiblesse qui ne lui permet pas d'exercer efficacement ses droits. Souvent, lorsque la justice intervient, l'atteinte est déjà consommée et ne peut plus être empêchée. Dans certains cas, la personne concernée n'obtient pas du maître du fichier les informations nécessaires pour pouvoir exercer ses prétentions, en particulier celles qui concernent les motifs justificatifs du traitement. L'obligation d'informer lors de la collecte n'a de sens que si elle s'accompagne de la possibilité pour la personne concernée de s'opposer efficacement au traitement. C'est pourquoi le projet prévoit la suspension immédiate, mais limitée à un bref laps de temps, du traitement en cas d'opposition de la personne concernée et l'obligation pour le maître du fichier de communiquer à cette dernière les motifs justificatifs du traitement. Le maître du fichier peut toutefois poursuivre le traitement si celui-ci repose sur une obligation légale.

On pourrait envisager d'autres mesures pour renforcer la position de la personne concernée dans le procès. On a pensé par exemple introduire l'idée d'un allégement du fardeau de la preuve, analogue à l'art.13*a* de la loi fédérale contre la concurrence déloyale[7]. Apporter la preuve de l'illicéité de l'atteinte ou de l'étendue du préjudice subi, par exemple lors d'une communication transfrontière de données, n'est en effet pas aisé. Il convient cependant de ne pas multiplier les exceptions au régime ordinaire de l'administration de la preuve. Même sans introduire d'allégement, la charge d'apporter la preuve de faits qui relèvent de la sphère d'influence du maître du fichier, comme l'existence de motifs justificatifs, devrait aujourd'hui déjà incomber au maître du fichier. Il s'est posé la question de savoir si les normes usuelles sur la responsabilité civile permettaient véritablement d'assurer la réparation du préjudice subi en cas d'atteinte illicite, notamment lors de la communication transfrontière des données. L'introduction de nouvelles sanctions, par exemple sous la forme d'une indemnité versée indépendamment du montant du préjudice subi, comme cela se fait lors de la résiliation abusive du contrat de travail, a été envisagée, mais n'a pas été retenue. Ce type de sanction est étranger au droit suisse, particulièrement dans un domaine qui n'est pas toujours régi par des rapports contractuels.

La révision permet de rapprocher le droit suisse sur certains points du droit communautaire, mais le projet n'a pas pour but de rendre notre droit en tous points compatible avec celui-ci. Il est admis que le niveau de protection offert par la LPD est à peu près équivalent à celui du droit communautaire. L'Union européenne a de plus rangé la Suisse dans le groupe des pays qui jouissent d'un niveau de protection adéquat, autorisant ainsi le transfert de données des pays de l'Union européenne vers notre pays. Dans le cadre des Bilatérales II, une révision plus étendue sera nécessaire. Elle pourrait intervenir lors d'une deuxième phase ou faire l'objet d'un message complémentaire adressé aux Chambres fédérales.

7 RS **241**

Sur le plan terminologique enfin, la LPD ne donne pas entière satisfaction. Certaines notions pourraient être définies (p. ex. les «tiers» ou la «procédure d'appel») et le terme «maître du fichier» ne correspond pas à la terminologie employée sur le plan communautaire. En raison des incidences en cascades que de nouvelles définitions légales auraient sur l'ensemble du texte de loi, il est préférable de renoncer à réviser ou à compléter les définitions actuellement prévues à l'art. 3 LPD dans le cadre d'une révision partielle.

1.2.2 Principales innovations

1.2.2.1 Devoir d'informer lors de la collecte des données personnelles

L'une des principales innovations du projet porte sur la réalisation de la motion «Renforcement de la transparence». Un devoir d'informer relativement détaillé est introduit lors de la collecte de données sensibles et de profils de la personnalité (art. 7*a*). Si les données collectées ne sont pas sensibles et ne constituent pas des profils de la personnalité, ce devoir est en revanche relatif. L'art. 4, al. 4, se limite, pour ce type de données, à poser le principe selon lequel la collecte, et notamment les finalités du traitement, doivent être reconnaissables. Ce principe n'est pas nouveau puisqu'il s'applique déjà à la collecte de données personnelles par des organes fédéraux (art. 18, al. 2, LPD). Il s'appliquera désormais également au secteur privé. L'étendue de cette obligation devra être appréciée en fonction des circonstances de la collecte. Si les circonstances sont telles que la collecte et la finalité du traitement sont d'emblée manifestement reconnaissables pour la personne concernée, aucun devoir d'information supplémentaire ne sera exigé de celui qui collecte les données. Par contre, si les circonstances sont telles que la collecte et la finalité du traitement ne sont pas ou pas clairement reconnaissables, on attendra de celui qui collecte des données qu'il informe la personne concernée de manière plus active.

1.2.2.2 Simplification de l'obligation de déclarer

L'obligation actuelle pour les personnes privées et les organes fédéraux de déclarer préalablement au Préposé toute communication de données personnelles (art. 6 LPD) est remplacée par une obligation de diligence qui ne comprend plus qu'une obligation restreinte d'informer. L'obligation pour les personnes privées de déclarer leurs fichiers au Préposé, lorsqu'elles traitent régulièrement des données personnelles sensibles ou des profils de la personnalité ou lorsqu'elles communiquent régulièrement des données personnelles à des tiers (art. 11 LPD), est maintenue à l'art. 11*a*. La proposition de l'avant-projet (supprimer l'obligation de déclarer), n'a pas eu l'écho escompté; en outre, il ne paraît plus à ce jour vraisemblable que l'Union européenne modifiera sa directive à ce sujet, comme c'était le cas au moment de l'élaboration de l'avant-projet. L'obligation de déclarer est donc maintenue, mais elle est réglée différemment; la déclaration en elle-même doit être simplifiée du point de vue administratif.

1.2.2.3 Procédure d'opposition

Le droit de la personne concernée de s'opposer à ce que des personnes privées traitent des données personnelles la concernant, est réglée à l'art. 12, al. 2, let. b, LPD; lorsque des données sont communiquées par des organes fédéraux, la personne concernée peut s'opposer à cette communication en vertu de l'art. 20 LPD. L'art. 15 LPD décrit la voie à suivre pour intenter action en justice contre un traitement effectué par des personnes privées. Le projet prévoit une nouveauté à l'art. 15*a*. Si la personne concernée s'oppose à un traitement de données, le maître du fichier a l'obligation de suspendre immédiatement celui-ci, à moins que le traitement mis en cause ne repose sur une obligation légale. S'il rejette l'opposition, le maître du fichier doit faire valoir un motif justificatif dans un délai de dix jours. S'il fournit un motif dans le délai légal imparti, la personne concernée peut se prévaloir de l'art. 15, al. 1, LPD en requérant du juge dans un délai de dix jours qu'il interdise provisoirement ou définitivement le traitement mis en cause. Cette mesure découle indirectement de la motion «Renforcement de la transparence». Le droit à être informé ne serait d'aucune utilité si la personne concernée ne pouvait pas s'opposer efficacement au traitement.

1.2.2.4 Encouragement de l'auto-réglementation par le biais de procédures de certification

Le projet encourage l'auto-réglementation dans le domaine de la protection des données. Il prévoit donc un nouvel art. 11 qui favorise le recours à des procédures de certification et à des labels de qualité et qui autorise le Conseil fédéral à réglementer si nécessaire la procédure et la reconnaissance d'organismes compétents en matière de protection. A titre de corollaire, l'art. 11*a* délie le maître du fichier de l'obligation de déclarer, s'il a obtenu une certification.

1.2.2.5 Mise en place de liaisons online avant l'adoption d'une base légale formelle

Dans sa réponse à la motion «Liaisons online», le Conseil fédéral a préconisé d'adapter les exigences de la LPD en matière de légalité en tenant compte des besoins pratiques. Le projet prévoit donc un nouvel art. 17*a* qui permet au Conseil fédéral d'autoriser, pour une durée limitée, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre de projets pilotes, avant que la base légale formelle y relative n'entre en vigueur. La loi énumère les critères qui déterminent dans quels cas l'exécution d'un projet pilote est indispensable. Les tâches qui nécessitent un traitement automatisé doivent, quant à elles, avoir une base légale formelle, comme c'est le cas déjà aujourd'hui.

1.2.2.6 Traitement conjoint de données personnelles par des organes fédéraux et des tiers

Il arrive que des organes fédéraux traitent des données conjointement avec des organes cantonaux, voire avec des personnes privées, lesquels à leur tour peuvent confier tout ou partie du traitement à des tiers. Se pose alors le problème de savoir comment l'organe fédéral peut continuer à assumer sa responsabilité dans ce domaine. Le projet améliore la protection des données sur ce point, car il permet à l'organe fédéral d'effectuer ou de faire effectuer des contrôles auprès de celui qui traite des données (art. 16, al. 3 et 4, du projet). La compétence d'effectuer des contrôles auprès des cantons ou de tiers découle aujourd'hui déjà de la fonction du maître du fichier. Elle résulte également des règles générales relatives à la compétence de la Confédération en matière de surveillance.

1.2.2.7 Standard minimum applicable aux cantons

Le projet renforce la protection des données lorsque celles-ci sont traitées par des organes cantonaux en exécution du droit fédéral en fixant un standard minimum tel que l'a réclamé la motion «Liaisons online». L'art. 37, al. 1, du projet s'inspire donc des règles applicables aux flux transfrontières, qui exigent la garantie d'un niveau de protection adéquat. Si les dispositions cantonales de protection des données n'assurent pas un niveau de protection adéquat, les dispositions du droit fédéral s'appliquent à titre supplétif.

1.2.3 Contexte international

1.2.3.1 Conseil de l'Europe

1.2.3.1.1 Droit en vigueur

Vu que le flux d'informations ne connaît pas de frontières, la coopération internationale est nécessaire pour assurer un niveau élevé de protection des données tout en garantissant la libre circulation des informations sans considérations de frontières. C'est dans cet esprit que le Conseil de l'Europe a adopté la Convention sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE n° 108) du 28 janvier 1981[8]. Cette Convention est entrée en vigueur pour la Suisse le 1er février 1998.

La Convention STE n° 108 a pour objet de renforcer dans les secteurs privé et public la protection juridique des individus vis-à-vis du traitement automatisé des données à caractère personnel les concernant. Elle tend à assurer, dans tous les Etats parties, un minimum de protection de la personnalité lors du traitement de données personnelles et une certaine harmonisation du système de protection; d'autre part, elle garantit la circulation internationale des données, en ce sens qu'aucun Etat partie ne peut interdire le transfert d'informations vers un autre Etat partie qui accorde la protection minimale prévue par elle.

8 RS **0.235.1**

Les principes de la protection des données énoncés dans la Convention STE n° 108 se retrouvent dans les lignes directrices de l'OCDE du 23 septembre 1980 régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel. Ils figurent également dans la Directive 95/46/CE (cf. ch. 1.2.3.2). La Convention STE n° 108 complète et concrétise, dans le domaine du traitement automatisé des données à caractère personnel, les art. 8 (droit au respect de la vie privée) et 10 (liberté d'expression) de la Convention du 4 novembre 1950 sur les Droits de l'homme et les libertés fondamentales (CEDH)[9], ratifiée par la Suisse le 28 novembre 1974. Le droit suisse satisfait déjà aux exigences de la Convention STE n° 108[10].

Le Comité des Ministres a adopté plusieurs recommandations en matière de protection des données. Ces recommandations prévoient généralement que celui qui collecte des données personnelles est tenu d'informer la personne concernée de manière appropriée. Les informations à donner concernent, selon les cas, notamment le fondement juridique de la collecte, les finalités pour lesquelles les données sont collectées et traitées, la catégorie des données collectées ou traitées, l'identité du responsable du traitement, des indications sur les personnes et organismes auprès desquels les données ont été collectées ou auxquelles les données peuvent être communiquées, le caractère facultatif ou obligatoire de la collecte, la possibilité de refuser son consentement et les conséquences d'un tel refus[11]. En réalisant la motion «Renforcement de la transparence» par l'introduction d'un devoir d'information détaillé pour les données sensibles et les profils de la personnalité et d'un devoir d'information plus relatif pour les autres catégories de données, le projet va dans le sens de ces recommandations.

1.2.3.1.2 Protocole additionnel à la Convention STE n° 108

Les Délégués des Ministres ont adopté, lors de leur réunion du 23 mai 2001, un Protocole additionnel concernant les autorités de contrôle et les flux transfrontières de données (Ci-après: Protocole additionnel). Ce Protocole complète la Convention STE n° 108 déjà ratifiée par la Suisse. Il a pour but de renforcer la mise en œuvre des principes contenus dans ladite Convention. Ce renforcement a été rendu nécessaire par le nombre croissant de flux transfrontières de données personnelles depuis un Etat partie à la Convention STE n° 108 vers un Etat ou une entité tiers. Il revêt deux aspects: d'une part il s'agit d'aller vers une harmonisation du fonctionnement et des compétences des autorités de contrôle, d'autre part d'éviter que des transferts de données à destination d'Etats ou d'entités tiers n'amènent à contourner la législation de l'Etat d'origine partie à la Convention STE n° 108.

9 RS **0.101**
10 RS **0.235.1**
11 Cf. ch. 3.2 de la Recommandation N° R (95) sur la protection des données à caractère personnel dans le domaine des services de télécommunications, eu égard notamment aux services téléphoniques; cf. ch. 5 de la Recommandation N° R (97) 5 relative à la protection des données médicales; cf. ch. 5 de la Recommandation N° R (97) 18 concernant la protection des données à caractère personnel, collectées et traitées à des fins statistiques; cf. ch. 3.3 de la Recommandation N° R (90) 19 sur la protection des données à caractère personnel utilisées à des fins de paiement et autres opérations connexes; cf. ch. 5 de la Recommandation N° R (2002) 9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

Le Protocole additionnel prévoit en particulier l'établissement d'autorités de contrôle qui sont chargées d'assurer le respect des mesures intégrant, dans le droit interne, des principes énoncés par lui et par la Convention STE. Ces autorités devront disposer du pouvoir d'investigation et d'intervention et du pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente les violations aux dispositions du droit interne qui donnent effet aux principes énoncés dans la Convention STE n° 108 et dans le Protocole additionnel. Ce dernier prévoit également que le transfert de données à caractère personnel vers un destinataire qui n'est pas régi par la Convention STE n° 108[12] ne peut être effectué que si l'Etat ou l'organisation destinataire assure un niveau de protection adéquat. Les garanties peuvent notamment résulter de clauses contractuelles, pour autant qu'elles soient jugées suffisantes.Tant sur la question des autorités de contrôle que sur celle des flux transfrontières, le Protocole additionnel prévoit un système qui est très proche de celui qui est prévu par la Directive 95/46/CE.

Le Protocole additionnel ne peut être signé que par les Etats signataires de la Convention STE n°108. Le nombre de ratifications nécessaires pour qu'il entre en vigueur a été fixé à cinq. Toute Partie peut, à tout moment, le dénoncer en adressant une notification au Secrétaire Général du Conseil de l'Europe.

Le 17 octobre 2002, le Conseil fédéral a signé ledit Protocole et propose au Parlement de l'approuver. A ce jour, deux Etats l'ont ratifié. Sa ratification permettra à la Suisse de se rapprocher du système mis en place par l'Union européenne et de signaler clairement sa volonté de respecter le niveau de protection garanti par le Conseil de l'Europe, notamment dans le domaine des flux transfrontières.

Concernant les incidences qu'aurait une ratification du Protocole additionnel en droit cantonal, il y a lieu de se référer au ch. 3.2.2.

1.2.3.1.2.1 Autorités de contrôle

Le Protocole additionnel oblige chaque Etat partie à prévoir une ou plusieurs autorités de contrôle indépendantes (art. 1, par. 1 et 3). Ces autorités doivent disposer du pouvoir d'investigation et d'intervention et du pouvoir d'ester en justice ou de porter les violations aux dispositions du droit interne donnant effet aux principes énoncés dans la Convention STE n°108 et dans le Protocole à la connaissance de l'autorité judiciaire compétente (art. 1, par. 2). Chaque autorité de contrôle doit en outre pouvoir être saisie par quiconque invoque la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel qui relèvent de sa compétence (art. 1, par. 2). Les décisions des autorités de contrôle peuvent à leur tour faire l'objet d'un recours juridictionnel (art. 1, par. 4). Les autorités de contrôle doivent en outre coopérer entre elles, notamment par l'échange d'informations (art. 1, par. 5).

La LPD prévoit déjà deux autorités de contrôle indépendantes, à savoir le Préposé qui s'acquitte de ses tâches de manière autonome (art. 26, al. 2, LPD) et la Commission fédérale de la protection des données, qui est une commission d'arbitrage et de recours au sens de la loi fédérale du 20 décembre 1968 sur la procédure administra-

12 RS **0.235.1**

tive[13] (art. 33 LPD). Il a des compétences d'investigation (art. 27, al. 1 à 3, et 29, al. 1 et 2, LPD) et des pouvoirs d'intervention, notamment celui d'émettre des recommandations (art. 27, al. 4 et 5, et 29, al. 3 et 4, LPD). Le Préposé peut intervenir d'office ou à la demande de tiers. Le droit en vigueur satisfait donc déjà très largement aux exigences du Protocole additionnel, à une exception près: le Préposé n'a actuellement pas la compétence d'ester en justice dans le cadre de sa mission de surveillance des organes fédéraux[14]. L'art. 27, al. 6, du projet permettra de rendre le droit suisse conforme au Protocole additionnel sur ce point.

1.2.3.1.2.2 Flux transfrontières

Le Protocole additionnel oblige les Etats parties à prévoir que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas partie à la Convention STE n° 108[15] ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré (art. 2, par. 1). Les Etats parties au Protocole additionnel peuvent toutefois autoriser dans leur législation interne des dérogations à ce principe pour des intérêts spécifiques de la personne concernée ou lorsque des intérêts légitimes prévalent, notamment des intérêts publics importants (art. 2, par. 2, let. a). De même, ils peuvent autoriser un transfert si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert et jugées suffisantes par les autorités compétentes (art. 2, par. 2, let. b).

Le caractère adéquat du niveau de protection doit être évalué à la lumière de l'ensemble des circonstances relatives au transfert et prendre en considération les principes de la Convention STE n°108 et du Protocole additionnel, ainsi que la manière dont ces principes sont respectés et dont la victime peut défendre ses intérêts en cas de non-conformité. Une évaluation peut être faite pour l'ensemble d'un Etat ou d'une organisation: dans ce cas, le niveau de protection est déterminé par les autorités compétentes de chaque Etat partie.

Les Etats parties possèdent une marge d'appréciation pour déterminer les dérogations au principe du niveau adéquat. De telles dérogations peuvent être prévues en vue de protéger un intérêt public important au sens de l'art. 8, par. 2, CEDH[16] et de l'art. 9, par. 2, de la Convention STE n° 108. Des exceptions peuvent également être prévues pour répondre à des intérêts spécifiques de la personne concernée, comme l'exécution d'un contrat, la protection de ses intérêts vitaux ou lorsqu'elle a donné son consentement.

La LPD règle déjà aujourd'hui le transfert de données personnelles à l'étranger. L'art. 6 LPD interdit la communication de données personnelles à l'étranger si la personnalité des personnes concernées s'en trouve gravement menacée, notamment du fait de l'absence d'une protection des données équivalente à celle garantie par la Suisse. D'autre part, quiconque entend transmettre des fichiers à l'étranger doit le déclarer préalablement au Préposé si la communication ne découle pas d'une obligation légale et qu'elle a lieu à l'insu des personnes concernées (art. 6, al. 2, LPD).

13 RS **172.021**
14 ATF **123** II 542
15 RS **0.235.1**
16 RS **0.101**

Le projet propose de remplacer cette obligation de déclarer par un système calqué sur celui du Protocole additionnel, lequel est analogue à celui de la Directive 95/46/CE.

1.2.3.2 Droit communautaire

La Directive 95/46/CE du Parlement et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Directive 95/46/CE) vise d'une part à garantir la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, et d'autre part à garantir la libre circulation des données à caractère personnel entre les Etats membres.

Par décision de la Commission du 26 juillet 2000[17], la Communauté européenne a rangé la Suisse parmi les Etats tiers qui offrent un niveau de protection adéquat aux fins de l'art. 25, par. 2, de la Directive 95/46/CE, attestant ainsi que, dans l'ensemble, la législation suisse offre un niveau de protection à peu près équivalent à celui de la Directive 95/46/CE. La LPD n'est toutefois pas en tout point compatible avec cette dernière.

Il serait prématuré d'entamer une révision totale de la LPD dans le but affirmé de la rendre entièrement compatible avec le droit communautaire (cf. ch. 1.2.1). Le projet rapproche cependant le droit suisse du droit communautaire sur différents points. En introduisant l'obligation d'informer lors de la collecte des données sensibles ou de profils de la personnalité (art. 7*a*), de même qu'en exigeant que la collecte soit reconnaissable pour la personne concernée dans les autres cas (art. 4, al. 4), le projet remplit en partie les exigences des art. 10 et 11 de la Directive 95/46/CE. Dans le domaine du consentement, l'art. 4, al. 5, du projet définit, de manière analogue à la Directive 95/46/CE, les conditions qui doivent être remplies pour que le consentement puisse être considéré comme valable. L'art. 7*b*, sans aller aussi loin que la Directive 95/46/CE, prévoit le droit pour les personnes concernées de ne pas être soumises à des décisions prises sur le seul fondement d'un traitement automatisé de données et permettra au moins de garantir que la personne concernée sera dûment informée du mode par lequel la décision aura été prise. Enfin, le projet prévoit de doter le Préposé de la qualité pour recourir contre les décisions des départements et de la Chancellerie fédérale (art. 27, al. 6). La Directive 95/46/CE prévoit en effet que chaque autorité de contrôle doit disposer du pouvoir d'ester en justice ou de porter les violations du droit interne à la connaissance de l'autorité judiciaire. Le Protocole additionnel prévoit une exigence analogue (cf. ch. 1.2.3.1.2).

Sur différents points, le projet ne va pas aussi loin que la Directive 95/46/CE. Cette dernière interdit en effet le traitement de données sensibles telles que l'origine raciale, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle des individus; cette interdiction n'est toutefois pas absolue puisqu'elle est assortie d'un certain nombre d'exceptions. Le droit suisse, quant à lui, considère ces données comme des données sensibles qui jouissent d'une protection particulière.

17 Publiée au JOCE n° L 215 du 25.8.2000, p. 1 ss.

Ainsi, la communication à des tiers de données sensibles ou de profils de la personnalité doit reposer sur l'un des motifs justificatifs énoncés à l'art. 13 LPD (cf. art. 12, al. 2, let. c, LPD). Le devoir d'information figurant à l'art. 7*a* du projet pour ce type de données devrait en outre avoir un effet dissuasif sur le maître du fichier, qui n'aura pas intérêt à collecter ce type de données si cela n'est pas strictement nécessaire à l'accomplissement de ses tâches. La Directive 95/46/CE prévoit de plus l'obligation pour le maître du fichier d'adresser une notification à l'autorité de contrôle avant la mise en œuvre d'un traitement entièrement ou partiellement automatisé. En droit suisse, l'obligation pour les personnes privées qui traitent des données d'annoncer les fichiers au Préposé est plus limitée que ne le prévoit la Directive 95/46/CE. Même si le projet prévoit quelques adaptations, celles-ci ne vont pas aussi loin que le devoir de notifier de la Directive 95/46/CE. A la différence du droit suisse, la Directive 95/46/CE prévoit que la personne concernée peut s'opposer à ce que des données la concernant soient traitées à des fins de prospection.

1.2.3.3 Comparaison internationale

1.2.3.3.1 Italie

Selon la loi n° 675 du 31 décembre 1996, les personnes concernées doivent être informées avant toute collecte, oralement ou par écrit, de la finalité et des modalités du traitement auxquelles les données sont destinées, du caractère obligatoire ou facultatif du traitement, des conséquences d'un éventuel refus de répondre, des destinataires ou catégories de destinataires auxquels des données peuvent être communiquées, des droits en matière d'information et d'accès, du nom et de la raison sociale du détenteur des données ou du responsable du traitement.

La loi italienne subordonne en principe le traitement de données par des personnes privées ou des organes publics au consentement exprès de la personne concernée, mais prévoit un certain nombre d'exceptions. La personne concernée a le droit de s'opposer, pour des motifs légitimes, au traitement des données qui la concernent, ainsi que le droit de s'opposer, sans avoir à invoquer aucun motif, à tout traitement de données à des fins commerciales ou de prospection.

L'organe de contrôle («il garante») est un collège composé de quatre membres élus par la Chambre des députés et le Sénat. Il jouit d'un statut d'autonomie. Il a notamment pour tâches de tenir le registre des fichiers, de contrôler l'application des dispositions légales, de signaler aux détenteurs de données et aux responsables du traitement les modifications à apporter pour assurer le respect de la protection des données, de se prononcer sur les recours déposés par les personnes concernées, de dénoncer les infractions poursuivies d'office et d'interdire les traitements susceptibles, en raison d'un risque concret, de porter préjudice à une ou plusieurs personnes. Il peut également prononcer des sanctions.

1.2.3.3.2 Allemagne

Le Bundestag a révisé la loi le 7 avril 2001 afin d'y transposer la Directive 95/46/CE. Cette révision vise notamment à renforcer la transparence à l'égard des personnes concernées. Lorsque des données sont collectées sans que la personne concernée en ait connaissance, le responsable du traitement doit l'informer de l'enregistrement des données, de la finalité de la collecte ou du traitement et de l'identité du responsable du traitement, ainsi que, dans le secteur privé, de la catégorie des données collectées. A moins que, compte tenu des circonstances, elle ne doive compter avec la communication des données à des tiers, la personne concernée doit également être informée des catégories de destinataires auxquels les données seront communiquées. Par ailleurs, les décisions ayant des conséquences juridiques pour un individu ou l'affectant de manière importante ne peuvent reposer exclusivement sur un traitement automatisé des données permettant d'évaluer certains aspects de sa personnalité.

1.2.3.3.3 Autriche

La loi sur la protection des données de 2000 impose au responsable du traitement un devoir d'information envers la personne concernée lors de la collecte de données. Ce devoir d'information est plus ou moins étendu selon les circonstances. Le responsable du traitement doit au moins lui fournir des informations sur la finalité du traitement et l'identité du responsable du traitement. Lorsque le principe de la bonne foi l'exige, d'autres informations doivent également lui être fournies, compte tenu des circonstances. Nul ne peut en outre être soumis aux effets d'une décision prise sur la seule base d'un traitement automatisé des données permettant d'évaluer certains aspects de sa personnalité, tels que sa performance au travail, son crédit, sa fiabilité ou son comportement.

La loi institue une commission («Datenschutzkommission») et un conseil («Datenschutzrat») de la protection des données. La commission est composée de six membres qui exercent leur fonction en toute indépendance. Tout traitement doit être notifié au préalable à la commission qui le consigne dans un registre. Quiconque se plaint d'une violation de ses droits peut s'adresser à la commission qui a le droit d'enquêter si elle a des raisons de présumer l'existence d'une violation de la loi. La commission peut émettre des recommandations. Si celles-ci ne sont pas suivies, elle peut, en fonction de la nature de la violation, déposer une plainte pénale, agir devant les tribunaux civils ou s'adresser à l'instance supérieure. Elle peut en outre être saisie par les personnes concernées en cas de violation du devoir d'information lors de la collecte.

1.2.3.3.4 France

La France n'a pas encore transposé la Directive 95/46/CE dans sa législation. La loi actuelle (loi 78/17) date du 6 janvier 1978. Un projet visant à transposer la Directive 95/46/CE est pendant auprès du Parlement.

La loi 78/17 instaure une Commission nationale de l'informatique et des libertés (CNIL) chargée de veiller au respect des dispositions de la loi. La CNIL est une autorité administrative indépendante qui dispose d'un pouvoir réglementaire. Elle est composée de dix-sept membres. La CNIL a pour tâches de recenser les fichiers, d'effectuer des contrôles sur place, d'établir des normes simplifiées afin que les traitements les plus courants et les moins dangereux fassent l'objet de formalités allégées, de garantir le droit d'accès, d'instruire les plaintes en privilégiant les règlements à l'amiable, d'informer et de conseiller.

Toute personne physique a le droit de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement. Des exceptions peuvent être prévues par la voie d'un acte réglementaire.

Les personnes auprès desquelles sont recueillies des informations nominatives doivent être informées du caractère obligatoire ou facultatif de leurs réponses, des conséquences à leur égard d'un défaut de réponse, des personnes physiques ou morales destinataires des informations et de l'existence d'un droit d'accès et de rectification. Lorsque les informations sont recueillies sur la base de questionnaires, ceux-ci doivent faire mention de ces prescriptions. De plus, aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

1.2.3.3.5 Royaume-Uni

La personne concernée peut s'opposer, par simple déclaration écrite auprès du responsable du traitement, à ce que des données personnelles soient traitées dans un but commercial et à ce qu'une décision l'affectant soit prise sur le seul fondement d'un traitement automatisé des données permettant d'évaluer certains aspects de sa personnalité, tels que son crédit, sa fiabilité, son comportement ou sa performance au travail. La personne concernée peut en outre s'opposer, par simple déclaration écrite et en invoquant des raisons spécifiques, à tout traitement susceptible de lui causer un préjudice substantiel. Le traitement de données sensibles est subordonné à son consentement. Aucun traitement ne doit en principe être effectué s'il n'a préalablement été annoncé par le responsable du traitement à l'organe de contrôle pour qu'il l'inscrive au registre des fichiers. Lors de la collecte et pour autant que cela soit possible, la personne concernée doit être informée de l'identité du responsable du traitement et de son représentant, de la finalité du traitement et de toute autre information nécessaire permettant d'assurer un traitement des données conforme à la bonne foi («to enable processing to be fair»).

L'organe de contrôle («Information Commissioner») a des tâches d'information et de conseil. Il peut édicter des codes de conduite. Il peut, d'office ou sur demande, prononcer une injonction («enforcement notice») envers toute personne qui contrevient aux principes de la protection des données. Le fait de ne pas suivre une injonction constitue une infraction.

1.2.4 Rapport avec d'autres projets législatifs

Actuellement, une loi fédérale sur la transparence de l'administration (loi sur la transparence) est en cours d'élaboration[18]. Cette loi crée un droit général à accéder aux documents officiels. Certaines dispositions de la LPD devront être adaptées à la lumière de cette nouvelle loi, afin que la coordination entre la protection des données personnelles et l'accès à l'information soit garantie. Il s'agit en particulier de compléter l'art. 19 en autorisant les autorités à accorder exceptionnellement l'accès à des documents officiels contenant des données personnelles à certaines conditions. De plus, une base légale devra également être créée afin de permettre aux autorités de publier sur Internet, dans le cadre de leur activité d'information, des documents comprenant non seulement des informations mais aussi des données personnelles (par exemple des rapports contenant des noms ou des adresses de particuliers).

D'autres dispositions devront être adaptées afin de garantir la coordination entre les règles de procédure prévues par la loi sur la transparence à celles de la LPD.

Dans le cadre des travaux préparatoires de la présente révision, il a été examiné de quelle manière la LPD, sa révision et la loi sur la transparence s'articulent entre elles, en particulier la question de la compatibilité des modifications de la LPD rendues nécessaires par la loi sur la transparence. Dans un souci de cohérence matérielle, ces dernières seront toutefois soumises au Parlement avec le projet de loi sur la transparence.

1.2.5 Procédure de consultation et résultats y relatifs

La consultation sur l'avant-projet et sur le Protocole additionnel à la Convention STE n° 108[19] a eu lieu entre septembre 2001 et janvier 2002.

Les objectifs principaux de la réforme ont reçu un large soutien, en particulier dans la mesure où ils répondent à la motion «Renforcement de la transparence». Seize cantons, cinq partis politiques (le Parti Radical Démocratique, les Jeunes Radicaux Suisses, le Parti libéral suisse, le Parti socialiste suisse et l'Union Démocratique du Centre) et quatorze organisations sont favorables à l'ensemble de la révision proposée. En revanche, les milieux économiques rejettent tout ou partie des propositions de révision. Ils craignent une charge de travail disproportionnée et des difficultés pratiques. La question de savoir si le domaine de la protection des données nécessite d'autres réformes ne fait pas l'unanimité. Certains participants à la consultation – notamment quelques cantons – estiment que la révision partielle proposée constitue une solution minimale, alors que d'autres souhaiteraient limiter strictement la révision aux questions abordées dans les deux motions.

L'introduction d'un droit de recours pour le Préposé, l'amélioration de la position de la personne concernée qui entend s'opposer au traitement de données la concernant, ainsi que la fixation d'un standard minimum pour les prescriptions des cantons en matière de protection des données ont été accueillis en majorité favorablement.

18 Cf. le message du 12 février 2003 relatif à la loi fédérale sur la transparence de l'administration.
19 RS **0.235.1**

En revanche, la proposition d'assouplir l'exigence selon laquelle le traitement de données par des organes fédéraux doit reposer sur une base légale formelle a été contestée. En outre, les avis sont controversés sur la question de supprimer l'obligation pour les personnes privées de déclarer leurs fichiers et sur la compétence du Préposé d'exécuter des contrôles auprès des cantons lorsque les autorités cantonales et les organes fédéraux traitent conjointement des données personnelles.

Enfin, la signature du Protocole additionnel à la Convention STE n° 108[20] n'a presque pas été critiquée.

1.2.6 Principales modifications par rapport à l'avant-projet

Le projet a été remanié à la suite de la procédure de consultation sur les points suivants:

- la communication de données à une société étrangère appartenant au même groupe de sociétés est simplifiée à certaines conditions si la société étrangère destinataire a son siège dans un Etat qui ne dispose pas d'une législation garantissant une protection appropriée des données (art. 6, al. 2, let. g,);
- il est proposé d'introduire une disposition sur la procédure de certification (label de qualité de protection des données [art. 11]);
- l'obligation de déclarer les fichiers est maintenue dans une forme adaptée (art. 11*a*);
- les conditions à remplir pour autoriser un traitement automatisé de données sensibles ou de profils de la personnalité avant l'entrée en vigueur d'une base légale formelle, sont modifiées (art. 17*a*);
- la compétence du Préposé d'exécuter des contrôles auprès des autorités cantonales lorsque celles-ci traitent conjointement des données avec des organes fédéraux est supprimée.

1.3 Mise en œuvre de la révision

Aucune mesure de mise en œuvre importante n'est nécessaire en droit public, du moins en ce qui concerne les autorités fédérales. La Confédération ne devra pas non plus prendre de mesures particulières par rapport au droit privé. Il incombera aux maîtres de fichiers privés de faire le nécessaire, notamment pour respecter leur nouveau devoir d'informer. La mise en œuvre de la révision dans le domaine du droit privé fera l'objet d'une surveillance de la part du Préposé en vertu de l'art. 29 LPD.

L'objectif visé par le projet qui consiste à favoriser l'auto-réglementation et en particulier la procédure de certification encouragera les maîtres de fichiers privés à se conformer à la révision partielle, ainsi qu'à la législation sur la protection des données. De plus, la simplification de la procédure de sauvegarde des droits des

20 RS **0.235.1**

personnes concernées devrait inciter les maîtres de fichiers privés à respecter les exigences supplémentaires introduites par la révision partielle.

Quant aux législations cantonales, elles devront être adaptées, dans la mesure où elles n'ont pas encore atteint un niveau de protection adéquat.

1.4 Classement des interventions parlementaires

Le projet réalise la motion 00.3000 de la Commission des affaires juridiques du Conseil des Etats du 28 janvier 2002 («Renforcement de la transparence lors de la collecte de données personnelles») et la motion 983529 de la Commission de gestion du Conseil des Etats du 17 novembre 1998 («Liaisons online. Renforcer la protection pour les données personnelles»). Les deux motions peuvent donc être classées (voir ch. 1.1.2).

2 Partie spéciale

2.1 Art. 2 Champ d'application

Il n'y a aucune raison de traiter de manière différente le Comité international de la Croix-Rouge des autres organisations internationales établies sur le territoire de la Confédération avec lesquelles un accord de siège a été conclu. En effet, les organisations internationales, en tant que sujets de droit international public, ne peuvent être sans autre soumises au droit suisse. En excluant expressément du champ d'application de la loi l'ensemble des organisations internationales, le projet est plus proche de la réalité. Le Comité international de la Croix-Rouge étant assimilé à une organisation internationale[21], il est couvert par cette exception.

L'art. 3, par. 2, let. a, de la Convention STE n° 108[22] donne la possibilité aux Etats signataires de soustraire du champ d'application de la Convention certains fichiers qui ne seraient pas soumis par le droit interne aux dispositions de protection des données. La Suisse a fait usage de cette possibilité et fait une telle déclaration lorsqu'elle a déposé l'instrument de ratification de la Convention STE n° 108, le 2 octobre 1997. La modification de l'art. 2, al. 2, let. e, nécessitera une nouvelle déclaration de sa part, dans laquelle elle notifiera au Secrétaire général du Conseil de l'Europe qu'elle ajoute les fichiers concernés à la liste des fichiers échappant au champ d'application de la Convention n° 108.

21 FF **1988** II 447 ss; cf. également U. Maurer / N. P. Vogt, Kommentar zum Schweizerischen Datenschutzgesetz, ad art. 2, al. 2, let. e, § 58 ss.

22 RS **0.235.1**

2.2 Art. 3 Définitions

La let. k devient la let. j. Le ch. 1 est adapté à la nouvelle Constitution fédérale du 18 avril 1999[23] (Cst.), qui, aux art. 163, al. 1, et 164, ne prévoit plus que deux formes d'actes édictés par l'Assemblée fédérale qui contiennent des règles de droit, à savoir la loi fédérale et l'ordonnance. Le ch. 2 reste inchangé.

2.3 Art. 4 Principes

Licéité du traitement (al. 1)

La formulation actuelle de l'art. 4, al. 1, LPD n'est pas tout à fait conforme à l'art. 5, let. a, de la Convention STE n° 108. Ce n'est pas uniquement la collecte qui doit être licite, mais tout traitement.

Le caractère reconnaissable de la collecte (al. 4)

L'art. 4, al. 4, du projet contribue à la réalisation de la motion «Renforcement de la transparence». Il pose le principe selon lequel la collecte doit être reconnaissable pour la personne concernée, notamment ses finalités. Ce principe général est complété par un devoir d'information plus détaillé, à l'art. 7*a*, pour les données personnelles sensibles et les profils de la personnalité.

Le devoir d'information visé à l'art. 7*a* et qui aurait valu pour la collecte de *toutes* les données personnelles n'a pas été retenu, bien qu'il soit plus conforme au droit européen et notamment aux recommandations du Conseil de l'Europe. Il avait également la faveur du Préposé. Au sein du groupe de travail qui a participé à l'élaboration de l'avant-projet, on a craint d'imposer une contrainte excessive aux maîtres de fichiers. C'est pourquoi on a jugé préférable, comme le réclame du reste la motion, de limiter le devoir d'information au traitement des données sensibles et des profils de la personnalité et d'exiger au surplus que la collecte soit reconnaissable. L'art. 4, al. 4, du projet constitue donc une amélioration de la situation actuelle sur le plan de la transparence, sans aller aussi loin que l'art. 7*a*. L'exigence du caractère reconnaissable de la collecte est déjà prévue à l'art. 18, al. 2, LPD pour les organes fédéraux; elle est simplement étendue aux personnes privées. Il convient en outre d'observer que certaines entreprises ont déjà pris les mesures nécessaires, sachant qu'il est dans leur intérêt d'être aussi transparentes que possible lors de la collecte de données personnelles si elles entendent gagner la confiance des consommateurs. A cet égard, la transparence exigée par le projet constitue un minimum. Les entreprises sont libres d'aller plus loin et d'appliquer le devoir d'information de l'art. 7*a* à toutes les données personnelles.

Les exigences qui devront être remplies pour qu'une collecte soit «reconnaissable» seront déterminées par les circonstances et conformes aux principes de la proportionnalité et de la bonne foi (art. 4, al. 2, LPD). Il s'agira donc, dans la pratique, de développer les critères adaptés à chaque cas. Il conviendra en particulier d'examiner dans une situation donnée quelles informations la bonne foi exigera que le maître du

[23] RS **101**

fichier fournisse à la personne concernée. Ces informations ne porteront pas seulement sur la collecte mais aussi sur certains de ses éléments déterminants, comme sa finalité, l'identité du maître du fichier ou les catégories de destinataires possibles des données si leur communication est envisagée. Dans certains cas, il pourra être nécessaire d'attirer l'attention de la personne concernée sur le caractère facultatif ou obligatoire des réponses données aux questions posées, de même que sur les conséquences du refus de répondre. Il est à noter que dans d'autres situations, l'information pourra être moins expresse et complète si le caractère reconnaissable de la collecte ressort des circonstances.

Exemples:

- Lorsque le client d'un grand magasin demande une carte de fidélité et qu'il doit alors fournir des données sur sa personne, il est généralement admis que le magasin pourra utiliser ces données pour lui envoyer sa publicité. En revanche si des données sur ses habitudes de consommation sont collectées lorsqu'il utilise sa carte, qu'elles sont utilisées pour établir un profil de consommation ou qu'elles sont vendues à des tiers, le client doit être rendu attentif de ce fait de manière appropriée (par exemple au moyen d'une remarque sur le formulaire à remplir pour obtenir une carte de fidélité).
- Si une personne réserve une chambre d'hôtel et qu'elle doit alors fournir des données personnelles qui sont en relation avec cette réservation (adresse, nombre de nuits, numéro de la carte de crédit etc.), l'hôtelier n'aura pas d'obligation particulière d'informer son client (à condition toutefois qu'il ne transmette pas ces données à des tiers), au motif que la collecte de ces données et le but poursuivi par l'hôtelier sont reconnaissables par le client.

Plus une transaction est complexe et plus la période pendant laquelle les données, suite à cette transaction, pourront être traitées est longue, plus les exigences quant au caractère reconnaissable de la collecte seront grandes. Il s'agira également d'examiner, sous l'angle du principe de la proportionnalité, dans quelle mesure il est nécessaire d'attirer l'attention de la personne concernée sur les éléments déterminants de la collecte, quels sont les moyens qui sont à la disposition du maître du fichier pour rendre ces éléments reconnaissables et dans quelle mesure on peut attendre de lui qu'il utilise ces moyens, eu égard notamment à leur coût et à leur efficacité. Les usages en vigueur dans la branche ou pour le type de transaction visé devront également être pris en compte. Pour des transactions simples de la vie quotidienne, dont les circonstances sont telles que la collecte, de même que sa finalité et l'identité du maître du fichier, sont d'emblée aisément et clairement reconnaissables pour la personne concernée, l'art. 4, al. 4, n'entraînera aucune obligation nouvelle pour le maître du fichier. Ainsi, on peut admettre que, pour la plupart des transactions courantes, l'application de l'art. 4, al. 4, ne posera aucun problème particulier. En revanche, moins les circonstances de la collecte rendent celle-ci reconnaissable, plus il sera nécessaire d'attirer l'attention de la personne concernée, par des moyens appropriés, sur l'existence de la collecte et ses éléments déterminants. Lors d'un sondage téléphonique, par exemple, une information donnée oralement sur les finalités de la collecte, l'utilisation des données et l'identité du maître du fichier, pourra suffire. Sur un site Internet, l'affichage à la page d'accueil, d'une rubrique suffisamment visible renvoyant à des informations concernant la collecte et l'utilisation des données constituera, dans la plupart des cas, un moyen simple et adéquat d'attirer l'attention de la personne concernée. D'autres moyens, comme la mention d'un avertissement sur un formulaire informant la personne concernée que, sauf opposition de sa part, les données seront communiquées à des tiers à des fins de prospection ou à d'autres fins peut tout à fait remplir son office sans être un effort

disproportionné pour le maître du fichier. Si la collecte est facultative, une clause permettant à la personne concernée de manifester son consentement, même si ce dernier n'est pas formellement requis par la loi, permettra également dans bien des cas d'éviter tout problème, le maître du fichier ayant alors l'assurance que la collecte était reconnaissable et que la personne concernée n'a pas manifesté l'intention de s'y opposer.

La collecte de données personnelles auprès d'un tiers doit également en principe être reconnaissable pour la personne concernée.

La transparence exigée par l'art. 4, al. 4, complétée par un devoir d'information plus étendu concernant les données sensibles et les profils de la personnalité à l'art. 7*a*, donne également une dimension nouvelle au droit de s'opposer au traitement, tel qu'il apparaît aux art. 12, al. 2, let. b, et 15 LPD. Le droit de s'opposer au traitement restait en effet largement théorique tant que les personnes concernées n'étaient pas conscientes de l'existence d'une collecte ni de ses éléments déterminants. La transparence de la collecte et l'information de la personne concernée constituent de ce point de vue la clef de voûte de tout le système de protection des données.

Il va de soi que le principe du caractère reconnaissable de la collecte est inapplicable lorsque, de par la loi, les autorités peuvent recueillir des données à l'insu de la personne concernée; à titre d'exemple on peut citer l'art. 14 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure[24] (LMSI).

Les conditions du consentement (al. 5)

Il convient de relever préalablement que l'art. 4, al. 5, ne modifie pas le droit actuellement en vigueur, mais qu'il clarifie la notion de «consentement».

La nécessité du consentement apparaît comme une condition du traitement des données à diverses reprises dans la LPD (art. 13, al. 1, art. 17, al. 2, let. c,) et dans le projet (art. 6, al. 2, let. b). La notion de «consentement» revêt une grande importance dans la pratique, car c'est l'un des motifs justificatifs le plus souvent invoqué par les personnes privées. Voilà pourquoi l'art. 4, al. 5, prévoit de clarifier cette notion en s'inspirant de la jurisprudence.

L'art. 4, al. 5, définit à quelles conditions le consentement donné doit être considéré comme valable. Il ne s'agit donc pas de faire du consentement une condition préalable à *tout* traitement de données ni d'introduire des exigences nouvelles par rapport au droit en vigueur. La notion de consentement valable s'inspire de celle de «consentement éclairé du patient»[25], dans le sens où la personne concernée doit disposer de tous les éléments du cas d'espèce qui lui permettent de prendre librement sa décision. Le terme «librement» correspond du reste au terme adopté par le droit communautaire. Cela signifie en particulier que la personne concernée doit être informée des conséquences ou des désavantages qui pourraient résulter pour elle d'un refus. Le fait qu'un refus entraîne un désavantage pour la personne concernée n'entache en revanche pas la validité même du consentement, sauf si ce désavantage est sans rapport avec le but du traitement ou qu'il est disproportionné par rapport à celui-ci. Ainsi, la personne qui consent au traitement de données personnelles la

24 RS **120**
25 Cf. notamment ATF **117** Ib 197, **114** Ia 350, c. 6, **119** II 456.

concernant pour permettre à un institut financier d'évaluer son crédit en vue de l'obtention d'une carte de crédit consent librement, même si elle sait qu'un refus la privera de la possibilité de se voir délivrer une telle carte. Dans une situation de ce genre, le désavantage qui résulte du non-consentement est en effet proportionné au but du traitement. Au contraire, le travailleur contraint de donner son consentement, sous la menace d'un licenciement, à un traitement de données qui n'est pas nécessaire à l'exécution du contrat de travail n'est pas en mesure de donner son consentement librement. En effet, le désavantage qui résulterait en pareil cas du refus de consentement serait manifestement disproportionné.

Le consentement n'est pas soumis à des règles de forme particulières et peut être implicite ou ressortir d'actes concluants, sauf s'il s'agit de données sensibles ou de profils de la personnalité. Conformément au principe de la proportionnalité, on considère aujourd'hui déjà que plus les données sont sensibles, plus le consentement doit être clair[26].

2.4 Art. 6 Communication transfrontière de données

L'obligation de déclarer au Préposé la communication de données à l'étranger n'a pas fait ses preuves dans la pratique. Peu d'entreprises font d'elles-mêmes la déclaration et le Préposé ne dispose pas des moyens nécessaires, notamment en personnel, pour effectuer des contrôles. C'est l'une des raisons pour lesquelles le projet abandonne cette obligation au profit d'un devoir de diligence imposé aux personnes privées et aux organes fédéraux qui transmettent des données à l'étranger.

Al. 1 et 2

Pour qu'une communication de données personnelles à l'étranger soit conforme à la loi, l'art. 6, al. 1, exige comme condition principale que la législation de l'Etat destinataire assure un niveau de protection adéquat. Cette disposition ne rend pas plus sévères les conditions prévues par le droit actuel qui exige un niveau de protection des données équivalente à celle qui est garantie en Suisse. L'al. 2 de cette disposition énumère la liste des conditions alternatives autorisant la communication de données personnelles à l'étranger, ce que le droit actuel ne fait pas. Le projet rend ainsi plus claires les différentes possibilités de garantir une communication conforme à la loi et laisse au maître du fichier la possibilité de choisir la solution qui lui convient. Contrairement au droit actuel qui emploie la notion de «transmission», le projet utilise le terme de «communication»; Il ne s'agit pas d'une modification matérielle, mais uniquement d'une unification de la terminologie à la lumière de l'art. 3.

La législation de l'Etat destinataire assure un «niveau de protection adéquat» lorsqu'elle répond aux exigences de la Convention STE n° 108[27]; de plus, il y a également lieu de tenir compte, dans la mesure du possible, de la manière dont est appli-

26 L. Brühwiler-Frésey, Medizinischer Behandlungsvertrag und Datenrecht, Zurich, 1996, p. 87.
27 RS **0.235.1**

quée la loi étrangère. Le Préposé tient une liste des Etats qui remplissent ces conditions.

Les personnes privées et les organes fédéraux qui transmettent des données à l'étranger devront s'assurer, par des moyens adéquats, que la transmission des données ne menace pas gravement la personnalité des personnes concernées. L'art. 6 instaure une protection assez semblable à celle qui est prévue par la Directive 95/46/CE. Il permet également de rendre le droit suisse conforme au Protocole additionnel à la Convention STE n°108 (cf. ch. 1.2.3.1.2).

Selon l'*art. 6, al. 2, let. a*, une communication à l'étranger est autorisée, nonobstant l'absence de législation étrangère assurant un niveau de protection adéquat, si des garanties suffisantes y remédient. Celles-ci peuvent résulter par exemple, d'un code de conduite, c'est-à-dire d'un ensemble de règles auxquelles les personnes privées peuvent se soumettre volontairement, tel que le «Safe Harbor Privacy Framework» qui a été négocié entre la Commission européenne et les Etats-Unis d'Amérique[28]. Celui qui transmet des données à l'étranger dispose à cet égard d'une grande marge de manœuvre, mais il est responsable du préjudice qui pourrait résulter d'une violation de l'obligation de diligence. Il incombe en principe à celui qui transmet des données à l'étranger de démontrer qu'il a pris toutes les mesures requises pour s'assurer d'un niveau de protection adéquat.

L'*al. 2* autorise à certaines conditions les flux transfrontières qui ne répondent pas aux exigences de l'al. 1. Les conditions posées aux let. a à g recouvrent en partie les motifs justificatifs de l'art. 13, al. 1 et 2, LPD. Contrairement aux intérêts prépondérants mentionnés à l'art. 13, al. 2, LPD, l'énumération des conditions figurant à l'art. 6, al. 2, est exhaustive. Il est à relever qu'il s'agit exclusivement de conditions alternatives.

L'*art. 6, al. 2, let. b*, s'applique à une situation concrète extra-contractuelle. Le terme «en l'espèce» doit être interprété de manière large, en ce sens qu'il ne vise pas forcément chaque opération de transmission particulière, mais peut au contraire se référer à un ensemble de communications. A titre d'exemple, la transmission de procès-verbaux tenus par des personnes composant un groupe de travail et se trouvant dans différents pays, est autorisée sans qu'il ne soit nécessaire de requérir le consentement de toutes les personnes concernées pour la communication de chaque document.

Dans le cadre d'une relation contractuelle, l'*al. 2, let. c*, prescrit que des données peuvent être communiquées à l'étranger si le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et que les données traitées concernent le cocontractant. Il est à noter que cette disposition ne s'applique que si la communication de données personnelles à l'étranger est indispensable pour la conclusion ou l'exécution d'un contrat.

L'*al. 2, let. e*, autorise la communication transfrontière de données si elle est, en l'espèce, nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée. Au sens de cette disposition, la communication est autorisée uniquement si elle tend à protéger un intérêt essentiel pour la vie de la personne concernée. La let. e vise donc la situation où la personne concernée n'est pas en mesure de faire valoir ses propres intérêts et qu'il peut être présumé de sa part qu'elle aurait don-

28 http://www.export.gov/safeharbor/sh_documents.html

né son accord à une telle communication. La notion de «protection de la vie ou de l'intégrité corporelle» correspond à celle de «sauvegarde de l'intérêt vital» adoptée par le droit communautaire (art. 26, par. 1, let. e, et par. 7, let. d, de la Directive 95/46/CE).

L'*al. 2, let. g*, prescrit que des données personnelles peuvent être communiquées à l'étranger si cette communication a lieu entre des personnes morales réunies sous une direction unique et soumises à des règles uniformes sur la protection des données garantissant une protection appropriée. La notion de «groupe de sociétés» correspond à celle de l'art. 663*e* , al. 1, du code des obligations[29]. La let. g de l'al. 2 répond ainsi en partie à la demande de différents milieux consultés qui voulaient qu'on prévoie une réglementation spéciale pour la communication de données au sein d'un groupe de sociétés.

Al. 3

Au niveau européen, il résulte de l'art. 2, par. 2, let. b, du Protocole que l'autorité compétente doit pouvoir examiner si les mesures de protection sont adéquates lorsque la législation de l'Etat destinataire n'offre pas une telle protection. C'est pourquoi la présente révision prévoit un devoir d'information.

Conformément à l'art. 6, al. 3, le maître du fichier doit informer le Préposé des garanties prises en vertu de l'art. 6 al. 2, let. a. En aucun cas, il n'a automatiquement l'obligation d'informer ce dernier de chaque communication particulière (par exemple des lettres et des courriers électroniques), comme le craignaient certains milieux consultés. Le Préposé doit également être informé des règles de protection des données adoptées lorsqu'en vertu de l'art. 6, al. 2, let. g, des données sont communiquées à une société appartenant à un même groupe de sociétés, qui a son siège dans un Etat étranger ne disposant pas d'une législation assurant un niveau de protection adéquat.

L'ordonnance du Conseil fédéral précisera au besoin à quel moment cette information devra être donnée et de quelle manière. La portée de l'obligation d'informer devra également être définie dans l'ordonnance. On pourrait par exemple prévoir qu'il n'y aura lieu d'informer le Préposé qu'une seule fois, soit lorsque le maître du fichier aura défini les règles générales et obligatoires applicables à toute communication transfrontière ou lorsqu'on aura recouru de manière régulière à certaines clauses contractuelles standards[30]. Lors d'un transfert de données au sein d'un groupe de sociétés, il n'y aura lieu d'informer qu'une fois le Préposé des règles de protection des données obligatoires pour les sociétés concernées. Il est à noter que la procédure d'information devra être aussi simple que possible et que par exemple le Préposé pourra être informé par courriel.

Le Préposé pourra, dans le cadre des pouvoirs d'investigation dont il dispose, établir au besoin si les garanties prises sont suffisantes (cf. art. 29, al. 1, let. d).

29 RS **220**

30 Voir par exemple les clauses contractuelles standards approuvées par la Commission européenne; décision 2001/497/CE du 15 juin 2001, Abl. L 181 du 4 juillet 2001, p. 19 ss, et décision 2002/16/EG du 27 décembre 2001, Abl. L 6 du 10 janvier 2002, p. 52 ss.

2.5 Art. 7*a* Devoir d'informer lors de la collecte de données personnelles sensibles et de profils de la personnalité

L'art. 7*a* prévoit l'obligation pour quiconque collecte des données sensibles ou des profils de la personnalité d'en informer la personne concernée. L'information doit être donnée d'office, ce qui distingue l'art. 7*a* du droit d'accès visé à l'art. 8. L'art. 9 permet au maître du fichier de refuser de donner l'information, de la restreindre, voire de la différer lorsqu'un intérêt public ou privé prépondérant l'exige.

L'art. 7*a* va plus loin que l'art. 4, al. 4, puisqu'il prévoit un véritable devoir d'information en se fondant sur la motion «Renforcement de la transparence». Une protection accrue est justifiée pour les données sensibles et les profils de la personnalité dans la mesure où le traitement de cette catégorie de données peut conduire à des discriminations. L'art. 7*a* devrait de ce point de vue avoir indirectement un effet préventif: s'il doit informer la personne concernée de manière plus étendue que pour d'autres types de données, le maître du fichier aura tout intérêt à s'abstenir de collecter, d'enregistrer ou de communiquer des données sensibles et des profils de la personnalité dont il n'a pas absolument besoin pour remplir ses tâches.

En vertu de l'al. 2, le maître du fichier doit – en règle générale de manière explicite – fournir à la personne concernée toutes les informations nécessaires pour que le traitement soit conforme aux principes de la bonne foi et de la proportionnalité, mais au minimum les informations qui figurent aux let. a à c, soit son identité, les finalités du traitement et les catégories de destinataires (mais non l'identité de chaque destinataire). Si le respect de la bonne foi l'exige, le maître du fichier devra fournir également d'autres informations, par exemple sur le caractère facultatif ou obligatoire de la collecte et sur les conséquences du refus de répondre aux questions (cf. commentaire de l'art. 4, al. 4).

Si une personne est déjà informée, qu'elle ait été informée une première fois par le maître du fichier ou qu'elle ait reçu l'information d'un tiers, le maître du fichier n'a pas besoin de l'informer à nouveau. L'information donnée lors de la première collecte n'a donc plus besoin d'être répétée à chaque fois si les circonstances des collectes subséquentes (à savoir notamment la finalité du traitement) sont couvertes par la première information.

L'information n'est soumise à aucune exigence de forme et peut donc être donnée oralement. La forme écrite est toutefois préconisée car il en restera une trace (preuve). L'information peut figurer sur un support écrit, qui peut être remis à la personne concernée ou placé à un endroit suffisamment visible (affichage, texte joint au contrat ou à la facture, rubrique apparaissant en bonne place sur la page d'accueil du site Internet, etc.). Comme pour l'art. 4, al. 4, le maître du fichier doit s'acquitter du devoir d'information visé à l'art. 7*a* dans le respect du principe de la proportionnalité et du principe de la bonne foi (art. 4, al. 2, LPD). L'information doit donc être suffisamment visible, lisible et intelligible. Le maître du fichier peut profiter de l'occasion pour coupler l'information avec la poursuite d'un autre objectif. Si la communication des données personnelles à des tiers est envisagée et que cette communication n'est ni obligatoire ni nécessaire à l'exécution d'un contrat, l'attention de la personne concernée peut être attirée au moyen d'une clause par laquelle elle est invitée à autoriser ou à refuser la communication: ce mode de faire permet

au maître du fichier de s'assurer que la personne concernée a reçu l'information et n'entend pas s'opposer ultérieurement à la communication des données (art. 12, al. 2, LPD). Il appartiendra aux praticiens, dans chaque domaine, de développer les moyens adéquats d'assurer l'information des personnes concernées, compte tenu des circonstances et des usages de la branche. L'art. 7*a* laisse de ce point de vue une importante marge de manœuvre aux maîtres des fichiers. Ceux-ci disposeront d'un délai transitoire d'un an pour mettre en œuvre les mesures d'information nécessaires (cf. les dispositions transitoires).

Exemples:

- Une caisse-maladie doit expressément indiquer, par exemple dans un courrier ou dans le contrat à conclure avec l'assuré, comment elle utilisera les données personnelles fournies par ce dernier sur son état de santé.
- Si un médecin procède à un test HIV sur un patient, il doit informer ce dernier qu'il devra annoncer tout résultat positif à l'Office fédéral de la santé en vertu de la loi sur les épidémies[31]; il est à noter que si le patient a été informé en bonne et due forme, l'office n'est pas tenu de l'informer à son tour. Cette information pourra avoir lieu par exemple oralement, mais il est également pensable qu'elle soit contenue dans une brochure explicative concernant le SIDA, sous une forme suffisamment claire, ce qui signifie qu'elle ne devra pas être imprimée en petits caractères.

L'*al. 3* règle le cas où les données ne sont pas collectées auprès de la personne concernée, mais auprès de tiers: la personne concernée doit alors en être informée de préférence lors de la collecte des données, mais au plus tard lors de l'enregistrement de celles-ci ou de leur première communication à un tiers. La notion d'enregistrement ne comprend pas seulement l'acte technique d'enregistrer les données collectées par exemple dans un système informatique; elle inclut tout acte postérieur à la collecte qui prépare l'exploitation des données.

Le maître du fichier peut renoncer à informer la personne concernée s'il se limite à procéder à une collecte ou si les circonstances rendent l'information de la personne concernée impossible ou très difficile (par exemple si le maître du fichier n'a aucun moyen de contacter la personne concernée). Le maître du fichier doit néanmoins entreprendre les démarches qu'on peut raisonnablement attendre de lui, compte tenu des circonstances: il ne peut se contenter de présumer que l'information est impossible ou disproportionnée. Son comportement doit être examiné conformément au principe de la bonne foi et l'exception de l'al. 3 ne saurait être interprétée de manière extensive. Le maître du fichier peut également renoncer à informer la personne concernée si l'enregistrement ou la communication des données est expressément prévue par la loi.

Si, dans le cadre de l'application du droit fédéral, les cantons transmettent des données sensibles ou des profils de la personnalité aux autorités fédérales (par exemple lorsqu'ils communiquent des données sur les retraits du permis de conduire à l'Office fédéral des routes aux fins d'enregistrement dans le registre automatisé des mesures administratives selon l'art. 104*b* de la loi fédérale sur la circulation routière[32]), il leur incombe d'informer les personnes concernées; en revanche, les autorités fédérales ne sont pas tenues de les informer à leur tour (art. 7*a*, al. 3).

31 RS **810.101**
32 RS **741.01**

Lors de la consultation, différents milieux intéressés ont demandé que la transmission de données personnelles au sein d'un groupe de sociétés constitue expressément une exception aux règles applicables lors de communications à des tiers, notamment dans le cas de l'art. 7*a*, al. 3. Un certain allégement pour les communications transfrontières est donc prévu à l'art. 6, al. 2, let. g, (voir le commentaire de l'art. 6, al. 2, let. g). Prévoir une exception générale au devoir d'informer inscrit à l'art. 7*a* pour les communications au sein d'un groupe de sociétés irait en revanche à l'encontre de l'objectif de créer davantage de transparence pour les personnes concernées.

L'art. 9 prévoit des exceptions au devoir d'informer lorsque la loi le prescrit et lorsque les intérêts prépondérants de tiers l'exigent. Les organes fédéraux peuvent en outre refuser l'information si un intérêt public prépondérant l'exige, de même que si la communication risque de compromettre une instruction pénale ou une autre procédure d'instruction.

On notera que la Directive 95/46/CE, les recommandations du Conseil de l'Europe et les législations des pays qui entourent la Suisse prévoient un devoir d'information très semblable, mais dont la portée est plus étendue (cf. ch. 1.2.3).

Certaines entreprises ont déjà pris des mesures qui leur permettent de satisfaire aux exigences du devoir d'information tel qu'il est prévu par l'art. 7*a*. Il convient de rappeler qu'il est également dans l'intérêt des entreprises d'être aussi transparentes que possible lors de la collecte de données personnelles, si elles entendent gagner et garder la confiance des consommateurs. Cette constatation est particulièrement vraie pour le développement du commerce électronique.

Celui qui omet intentionnellement d'informer la personne concernée de la collecte ou qui ne lui fournit pas les informations prévues à l'al. 2, let. a à c, ou celui qui lui fournit intentionnellement des informations inexactes peut être poursuivi pénalement (art. 34, al. 1).

2.6 Art. 7*b* Devoir d'informer lors de décisions individuelles automatisées

L'art. 7*b* complète l'art. 7*a* par un devoir d'information particulier lorsqu'une décision produisant des effets juridiques ou affectant de manière significative la personne concernée est prise sur le seul fondement d'un traitement automatisé de données visant à évaluer certains aspects de sa personnalité. Il s'agit en l'occurrence d'éviter que l'évaluation de la personnalité de la personne concernée ne soit effectuée sur la seule base d'une décision automatisée, sans qu'une appréciation humaine intervienne et sans que la personne concernée soit informée de la manière dont la décision a été prise. De telles décisions servent à évaluer des aspects de la personnalité tels que le crédit, la fiabilité, le comportement ou les risques et se fondent sur des généralités statistiques (par ex. pour déterminer l'assurance responsabilité civile, la conductrice qui possède une petite voiture sera automatiquement rangée dans une classe de risque moins élevée que le conducteur qui possède une voiture de sport).

En prévoyant un simple devoir d'information, le projet ne veut pas aller aussi loin que la Directive 95/46/CE et que les législations des pays voisins, lesquelles reconnaissent à toute personne le droit de ne pas être soumise à une décision prise sur le

seul fondement d'un traitement automatisé de données, ce qui équivaut à garantir à la personne concernée une sorte de droit d'être entendu. Le devoir d'information prévu à l'art. 7*b* ne complique en aucune manière la tâche du maître du fichier, car il peut être concrétisé très simplement: il suffit de faire figurer sur la décision automatisée une phrase-type succincte. Bien qu'il ne soit pas expressément visé par la motion «Renforcement de la transparence», ce devoir d'information poursuit le même objectif.

Celui qui omet intentionnellement d'informer la personne concernée au sens de l'art. 7*b* peut être poursuivi pénalement (art. 34, al. 1).

2.7 Art. 8 Droit d'accès

L'art. 8 est complété à l'al. 2, let. a, par l'obligation de communiquer à la personne concernée les informations sur l'origine des données, pour autant que ces informations soient disponibles. La personne concernée peut en effet avoir un intérêt légitime à connaître l'origine des données, par exemple pour pouvoir remonter aux sources de la collecte et faire rectifier d'éventuelles erreurs. Cette exigence contribue à renforcer la transparence dans le sens de la motion adoptée par les Chambres et clarifie le droit d'accès. L'intérêt de la personne concernée à connaître les sources de l'information est déjà admis par la jurisprudence[33]. Cette précision peut également avoir un effet préventif, dans la mesure où celui qui collecte des données doit compter avec la possibilité pour la personne concernée d'être informée des origines de la collecte.

2.8 Art. 9 Restriction du devoir d'information et du droit d'accès

Les restrictions du droit d'accès ont été étendues au devoir d'information de l'art. 7*a*. Il se peut en effet qu'en raison d'un intérêt public ou privé prépondérant le maître du fichier ne puisse donner l'information prévue à l'art. 7*a* ou qu'il soit obligé de la différer. Du fait que les motifs de restriction sont identiques à ceux du droit d'accès, l'application de cette disposition dans le cadre du devoir d'information de l'art. 7*a* ne devrait pas poser de problème particulier. Si le maître du fichier rejette, restreint ou diffère l'information, il doit en informer la personne concernée dès que le motif de restriction a disparu, pour autant que cela n'entraîne pas d'efforts disproportionnés (art. 9, al. 5, du projet; cf. également art. 18, al. 6, LMSI[34]).

33 Cf. arrêt non publié du Tribunal fédéral du 18 septembre 1991, Dr F contre le gouvernement du canton de Saint-Gall, c. 5a; cf. également, dans le domaine pénal, ATF **118** Ia 457.

34 RS **120**

2.9 Art. 10*a* Traitement de données par un tiers

L'art. 14 LPD a été déplacé dans la partie générale et devient l'art. 10*a*. Il ne s'applique actuellement qu'au traitement des données par des personnes privées. La LPD ne contient pas de disposition semblable pour le traitement des données par des organes fédéraux. De par son transfert dans la partie générale, cet article s'appliquera non seulement aux personnes privées, mais aussi aux organes fédéraux et, à titre supplétif, aux organes cantonaux qui traitent des données en exécution du droit fédéral (art. 37, al. 1).

Le traitement de données ne peut être confié à un tiers que si la sécurité des données est assurée (al. 2). Cette exigence découle – entre autres – des recommandations émises par la Commission de gestion du Conseil des Etats[35]. Lors de la consultation, divers milieux concernés avaient demandé qu'on concrétise les modalités de cette exigence en les définissant dans la loi. Si des règles d'organisation techniques supplémentaires sont nécessaires, elles seront édictées dans le cadre de l'ordonnance. Il convient du reste de relever que le mandataire a l'obligation de respecter les mêmes normes que le mandant en matière de sécurité des données (voir en particulier l'ordonnance du 14 juin 1993 relative à la LPD; OLPD[36]).

Pour ce qui est de la portée de l'obligation de diligence du mandant, l'*al. 2* ne déroge pas au droit en vigueur. Toutefois, il met plus clairement en évidence cette obligation du mandant et la précise. Celui-ci doit s'assurer que le mandataire respecte le standard de sécurité nécessaire. Il peut également se baser sur le label de qualité sur la protection des données accordé au mandataire ou sur une procédure de certification effectuée par un organisme indépendant (voir le commentaire de l'art. 11). Il doit en particulier s'assurer que le mandataire fait effectivement usage de la norme de sécurité. Les autres modalités concernant en particulier le droit du mandant de donner des instructions au mandataire, le concept de sécurité et les mesures d'organisation techniques doivent être réglées dans l'ordonnance, pour autant que ces règles soient nécessaires en plus des normes existantes.

Les motifs justificatifs invoqués à l'al. 3 sont non seulement ceux de l'art. 13 LPD, mais aussi les bases juridiques au sens de l'art. 17 LPD, vu la portée générale de l'art. 10*a*.

Le maître du fichier répond du préjudice qu'il peut avoir causé en confiant le traitement à un tiers sans s'être assuré de la sécurité des données.

2.10 Art. 11 Procédure de certification

Une nouvelle disposition concernant l'auto-réglementation a été introduite dans le projet. Elle ne figurait pas dans l'avant-projet. La responsabilité du maître du fichier est ainsi renforcée et la concurrence est stimulée. Cela contribue à améliorer de manière continue la protection et la sécurité des données; cela corrige également les insuffisances de la loi actuelle. De plus, le concept d'auto-contrôle amène dans une

35 Cf. recommandation 267, Rapport de la Commission de gestion du Conseil des Etats du 19 novembre 1998, Mise en place de liaisons «Online» dans le domaine de la police; FF **1999** 5200, p. 5231.

36 RS **235.11**

certaine mesure à prendre en compte l'évolution technologique. L'absence de dispositions y relatives dans l'avant-projet a été critiquée par plusieurs milieux consultés. La présente disposition s'inspire de l'art. 43*a* de la loi fédérale sur la protection de l'environnement (LPE)[37], qui a donné de bons résultats dans la pratique.

L'*al. 1* consacre le principe de base. Le projet vise à encourager les procédures de certification aussi bien des processus d'exploitation et des structures d'organisation (certification de la protection des données) que des systèmes techniques d'informatique ou de programmes, c'est-à-dire de produits. Lorsqu'il a été constaté dans le cadre d'une procédure de certification que les normes légales et techniques ont été respectées, un label de qualité de la protection des données doit être attribué. Cette distinction peut être utilisée par des entreprises certifiées notamment à des fins publicitaires et donc portée à la connaissance du public. Les autorités et les sociétés certifiées ne sont alors plus tenues de déclarer leurs fichiers conformément à l'art. 11*a*, al. 2 et 3, si le résultat de la procédure de certification a été communiqué au Préposé (art. 11*a*, al. 5, let. f). Cet allégement est une mesure incitative.

Les organismes de certification doivent être indépendants des personnes privées et des autorités à évaluer, surtout sur le plan organisationnel, mais aussi dans les faits. Leur reconnaissance sera réglementée par le Conseil fédéral dans une ordonnance (al. 2). Il est éventuellement possible de prévoir que les organismes de certification doivent être accrédités[38]. De plus, il incombe au Préposé d'examiner si la procédure de certification et l'attribution d'un label de qualité sont compatibles avec le droit en vigueur (voir art. 31, al. 1, let. f). Il peut utiliser les instruments prévus par la LPD et notamment émettre des recommandations (voir le commentaire de l'art. 29 LPD). Il ne fonctionnera toutefois pas en tant qu'autorité de certification.

Aujourd'hui, il est possible d'obtenir en Suisse un label de qualité de la protection des données; des entreprises se sont déjà soumises à des procédures de certification. Un instrument de qualification a également été développé en Allemagne; il est actuellement testé.

2.11 Art. 11*a* Registre des fichiers

A l'heure actuelle, les personnes privées sont, conformément à l'art. 11, al. 3, let. b, LPD, tenues de déclarer leurs fichiers si les personnes concernées n'ont pas eu connaissance du traitement des données les concernant. Or, avec l'obligation de rendre la collecte reconnaissable (art. 4, al. 4,) et le devoir d'informer lors de la collecte de données sensibles et de profils de la personnalité (art. 7*a*), la déclaration des fichiers perd de son importance.

L'avant-projet avait proposé la suppression de l'obligation pour les personnes privées de déclarer leurs fichiers. On voulait d'une part tenir compte du fait que la présente révision prévoit pour les personnes privées de nouvelles obligations d'informer. D'autre part, une modification du droit communautaire sur ce point semblait envisageable à l'époque. Or ce ne fut pas le cas. De plus, différents milieux consultés s'étaient opposés à la suppression de l'obligation de déclarer les fichiers. Voilà pourquoi ce devoir est maintenu, mais sans l'exception prévue à l'art. 11,

37 RS **814.01**
38 Voir art. 2 de l'ordonnance sur l'accréditation et la désignation; RS **946.512**

al. 3, let. b, de la loi actuelle. En revanche, l'obligation de déclarer les fichiers est assouplie par de nouvelles exceptions qui permettent aussi un certain rapprochement avec le droit communautaire.

Sur le plan administratif, la déclaration sera simplifiée par la mise à disposition de formulaires ad hoc sur Internet.

L'*art. 11a, al. 1*, fixe expressément le nouveau principe selon lequel le registre des fichiers doit pouvoir être consulté sur Internet. Des mesures allant dans ce sens sont en cours. La transparence s'en trouvera améliorée.

Le projet prévoit à *l'al. 3*, que les fichiers doivent être déclarés si des données sensibles ou des profils de la personnalité sont régulièrement traités ou si des données personnelles sont régulièrement communiquées à des tiers. Contrairement au droit en vigueur, les personnes privées sont tenues de déclarer leurs fichiers, même si les personnes concernées en sont informées.

L'*al. 4* prescrit expressément que les fichiers doivent être déclarés avant d'être opérationnels.

L'*al. 5* prévoit une série d'exceptions. Les organes fédéraux sont notamment traités de la même manière que les personnes privées. Il est à noter que la Directive 95/46/CE ne fait pas non plus de distinction entre les autorités et les personnes privées. Sur ce point, le projet se rapproche d'une certaine manière du droit communautaire.

Comme le droit en vigueur, l'*al. 5* prescrit que les personnes privées n'ont pas l'obligation de déclarer leurs fichiers si elles traitent des données en vertu d'une obligation légale; cet alinéa confère également au Conseil fédéral la faculté de prévoir des exceptions (let. a et b). A la différence du droit en vigueur qui prévoit des exceptions pour les médias à l'art. 4 LPD, le projet consacre celles-ci aux let. c et d, afin que l'al. 5 soit exhaustif.

La *let. e* prévoit une nouveauté qui rend compatible l'obligation de déclarer au système de déclaration adopté par la Directive 95/46/CE. Comme l'art. 11, cette disposition vise à encourager l'auto-réglementation. Le maître du fichier peut désigner un conseiller à la protection des données qui est chargé de tenir un inventaire des fichiers et de surveiller que du point de vue interne les conditions-cadres de la protection des données sont respectées. Le conseiller en matière de protection des données doit être indépendant sur le plan organisationnel, c'est-à-dire qu'il n'a pas l'obligation de s'en tenir aux instructions du maître du fichier et qu'il ne lui est pas subordonné. Selon l'*al. 6*, le Conseil fédéral règle les modalités du rôle et des tâches du conseiller à la protection des données. Il peut en particulier prévoir que sa nomination n'est valable que si elle a été annoncée au Préposé.

L'exception prévue à la *let. f*, est la conséquence du principe consistant à encourager le recours à des procédures de certification. Si le maître du fichier obtient un label de qualité, cela veut dire qu'il respecte les exigences légales. Le résultat de la procédure de certification doit être communiqué au Préposé. On assure ainsi qu'un contrôle peut avoir lieu si l'occasion se présente et que les personnes concernées peuvent demander au Préposé si une société a fait l'objet d'une procédure de certification. Ce dernier peut publier la liste des entreprises et autorités certifiées.

2.12 Art. 12 Atteintes à la personnalité

Le changement de système induit par la modification de l'art. 6 LPD entraîne la suppression du renvoi à l'art. 6, al. 1, qui figure actuellement à l'art. 12, al. 2, let. a.

Il découle de l'art. 12, al. 2, let. a, LPD que la communication de données personnelles à l'étranger est permise même en présence d'un risque de violation de la personnalité, dans la mesure où le maître du fichier peut invoquer un motif justificatif selon l'art. 13 LPD. A l'art. 6 du projet de révision, les motifs pouvant justifier une dérogation au principe de l'art. 6, al. 1, sont dorénavant énumérés de manière exhaustive à l'al. 2.

2.13 Art. 14 Traitement de données par un tiers

L'art. 14 est remplacé par l'art. 10*a*. Il est donc renvoyé au commentaire de l'art. 10*a* ci-dessus.

2.14 Art. 15 Prétentions et procédure

Le texte des al. 1 et 3, subit une modification d'ordre rédactionnel qui a pour effet de mettre davantage l'accent sur la possibilité pour le demandeur de requérir que le traitement des données, et non seulement leur communication à des tiers, soit interdit. Ce droit existe déjà (cf. art. 12, al. 2, let. b, en relation avec l'art. 15, al. 1, LPD). Toutefois, avec l'introduction d'un devoir d'information à l'art. 7*a* du projet, le droit de requérir l'interdiction du traitement deviendra plus effectif (cf. également commentaire de l'art.15*a*).

2.15 Art. 15*a* Opposition au traitement de données personnelles

Le droit de s'opposer au traitement des données sur le plan civil existe actuellement en vertu des art. 12, al. 2, let. b, et 15 LPD. L'art. 15*a* du projet ne fait que régler la procédure en renforçant modérément la position de la personne concernée. L'introduction de l'obligation d'informer à l'art. 7*a* risque d'avoir peu d'utilité si elle n'est pas assortie de la possibilité, pour la personne qui est informée de la collecte, de pouvoir s'opposer efficacement au traitement. D'autre part, le droit de s'opposer au traitement n'a véritablement de sens que si le traitement peut être suspendu avant qu'il ne cause un préjudice difficilement réparable à la personne concernée. Enfin, la personne concernée doit avoir connaissance des motifs du traitement pour pouvoir exercer ses droits au sens de l'art. 15 LPD.

La personne concernée ignore souvent si le traitement répond ou non à un motif justificatif au sens de l'art. 13 LPD et le maître du fichier n'a actuellement pas l'obligation de motiver le traitement. Elle peut certes demander au maître du fichier des explications, mais il n'est pas rare que ce genre de demande reste sans réponse. Dans ce cas, elle doit prendre le risque d'intenter une action au sens de l'art. 15 LPD sans savoir quelles sont ses chances de succès.

En vertu de l'art. 15*a*, al. 1, la personne concernée peut s'opposer au traitement de données la concernant en exigeant du maître du fichier qu'il le suspende immédiatement. Afin d'empêcher des abus de la part de la personne concernée, la disposition susmentionnée prévoit qu'un traitement qui repose sur une obligation légale ne doit pas être suspendu; dans ce cas, la personne concernée doit en être informée *immédiatement* (al. 3, 2e phrase). Pour pouvoir poursuivre le traitement, le maître du fichier doit, aussi vite que possible, communiquer à la personne concernée les motifs justificatifs sur lesquels il fonde son traitement; il dispose pour cela d'un délai de dix jours. Si le traitement n'est pas justifié, il peut renoncer à l'effectuer de sa propre initiative.

Sur la base des motifs justificatifs fournis par le maître du fichier conformément à l'art. 15*a*, *al. 3*, la personne concernée peut apprécier la licéité du traitement la concernant. Dans la plupart des cas, elle se satisfera de la réponse du maître du fichier et renoncera à intenter une action en justice. Il est donc dans l'intérêt des deux parties d'éviter des procédures inutiles. L'art. 15*a* y contribue, puisqu'il permet au maître du fichier de communiquer les motifs du traitement à la personne concernée et par conséquent de la convaincre du caractère justifié du traitement. Il permet également à la personne concernée de mieux évaluer les chances d'une action en justice.

Si la personne concernée n'est pas satisfaite des motifs justificatifs fournis par le maître du fichier, l'art. 15*a*, al. 5, prescrit qu'elle dispose d'un délai de dix jours pour intenter les actions prévues à l'art. 15 LPD et requérir des mesures provisionnelles; elle peut en particulier demander la rectification des données, leur destruction, ainsi que l'interdiction de leur communication ou de leur traitement.

L' *al. 4* décrit les effets de l'opposition à un traitement de données. Le maître du fichier a l'obligation de suspendre le traitement mis en cause; il est toutefois autorisé à conserver, à archiver ou à enregistrer les données en question jusqu'à droit connu, c'est-à-dire aussi longtemps que le délai pour la personne concernée d'intenter action coure et jusqu'à ce que, le cas échéant, le juge statue sur l'admissibilité du traitement mis en cause et que la décision soit devenue définitive. Si la personne concernée ne saisit pas le juge dans le délai, le maître du fichier peut, quel que soit le cas, poursuivre le traitement. Cette précision est nécessaire sachant que la notion de «traitement» au sens de l'art. 3, let. e, LPD comprend également les opérations mentionnées dans la présente disposition.

Si la personne concernée ne saisit pas la justice dans le délai légal, son opposition est réputée levée. Le maître du fichier est dès lors autorisé à poursuivre le traitement, ainsi que toutes les opérations y relatives. Le délai prévu à l'al. 5 limite donc uniquement la durée de l'interdiction du traitement au sens de cette disposition, et non pas le droit de la personne concernée de faire valoir ses droits en justice conformément à l'art. 15 LPD. En revanche, l'art. 15*a* ne pourra à nouveau être invoqué que si les conditions de fait ou de droit ont changé de manière déterminante; en l'absence d'un tel changement, il pourrait y avoir abus de droit de la part de la personne concernée.

L'*al. 6* prévoit expressément que la procédure de l'art. 15*a* n'est pas applicable aux médias à caractère périodique puisque ceux-ci doivent pouvoir coller à l'actualité. Cela signifie que les actions intentées contre un média à caractère périodique sont uniquement régies par l'art. 15 LPD.

2.16 Art. 16 Organe responsable

Deux nouveaux alinéas sont introduits à l'art. 16, qui permettent à l'organe fédéral responsable du traitement d'effectuer des contrôles lorsqu'il traite des données conjointement avec des organes cantonaux ou des personnes privées. Il peut arriver que des organes cantonaux, voire des personnes privées, traitent des données conjointement avec un organe fédéral sans que le traitement en question soit nécessairement lié à l'exécution du droit fédéral. Dans la mesure où il s'agit de banques de données fédérales, l'organe fédéral doit s'assurer que les données sont traitées de manière licite et compatible avec la LPD; il doit en particulier vérifier que la sécurité informatique est garantie. Si le traitement est effectué par des personnes privées ou à l'étranger, il est nécessaire de régler l'exécution des contrôles par convention. Lors des contrôles, l'organe fédéral collabore avec l'organe de contrôle cantonal.

2.17 Art. 17 Bases juridiques

L'al. 2 subit quelques modifications d'ordre mineur.

A la *let. b*, il est précisé que le Conseil fédéral peut exceptionnellement accorder une autorisation dans un cas d'espèce. Cette clause de délégation ne permet donc pas de délivrer des autorisations pour un nombre de cas indéterminé. C'est d'ailleurs ainsi qu'elle a toujours été interprétée jusqu'ici.

A la *let. c*, on tient compte du droit pour la personne concernée de s'opposer au traitement. Par analogie avec le secteur privé (art. 12, al. 3, LPD) et comme corollaire du devoir d'informer prévu à l'art. 7*a*, il est juste de donner plus de poids au droit, pour la personne concernée, de s'opposer au traitement, même si elle a rendu ses données accessibles à tout un chacun. Avec le développement d'Internet, le traitement de données personnelles sensibles a pris une dimension qui échappe à la maîtrise de la personne concernée et qui justifie que celle-ci puisse s'opposer au traitement quand bien même elle aurait rendu ses données accessibles à tout un chacun.

2.18 Art. 17*a* Traitement de données automatisé dans le cadre de systèmes pilotes

En réponse à la motion «liaisons online», le Conseil fédéral a préconisé d'adapter les exigences de la LPD en matière de légalité en tenant compte des besoins pratiques (cf. ch. 1.2.1.1).

L'avant-projet proposait de donner la faculté au Conseil fédéral d'autoriser le traitement automatisé de données sensibles ou de profils de la personnalité avant même l'entrée en vigueur d'une loi au sens formel. Suite aux critiques émises lors de la consultation, une autre solution, nettement plus restrictive, a été envisagée, permettant au Conseil fédéral d'autoriser uniquement la communication de données sensibles ou de profils de la personnalité par le biais d'une procédure d'appel. Cette variante minimale n'aurait toutefois pas permis de résoudre les problèmes qui se posent dans la pratique. Par conséquent, le choix s'est porté sur un instrument qui

reprend la première proposition, mais qui se limite à permettre au Conseil fédéral d'autoriser, pour une durée limitée, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre d'essais pilotes, avant que la base légale formelle y relative ne soit entrée en vigueur.

La mesure proposée va dans la direction des recommandations de la Commission de gestion du 19 novembre 1998[39], selon lesquelles le Conseil fédéral doit examiner les liaisons on-line, avant qu'elles ne soient réglées dans une loi formelle, sous l'angle de l'opportunité, de la proportionnalité et de la finalité. Du point de vue technique, la mise en place de nouvelles liaisons on-line n'est plus le vrai problème. La structure d'un système informatique doit plutôt, dès le début, être adaptée à ces liaisons. Ceci signifie en fin de compte qu'il ne suffit pas de pouvoir tester de nouvelles liaisons lors d'essais pilotes, mais qu'il est judicieux d'évaluer un système dans sa totalité dans le cadre d'un projet pilote.

Il convient de rappeler que, selon le droit en vigueur, des données sensibles ou des profils de la personnalité ne peuvent être traités que si une loi au sens formel le prévoit expressément ou, exceptionnellement, si l'une des conditions prévues à l'art. 17, al. 2, let. a à c, LPD est remplie. De plus, en vertu de l'art. 19, al. 3, LPD, les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément. Selon la loi actuelle, une base légale formelle régissant uniquement les tâches qui nécessitent le traitement n'est pas suffisante. Elle doit encore indiquer l'organe qui a accès aux données, la finalité pour laquelle l'accès est accordé et l'étendue de cet accès.

Les exigences envers la base légale régissant le traitement de données sensibles ou de profils de la personnalité sont très strictes. Ceci ne va pas sans poser problème: à défaut de tests d'accès à des banques de données effectués dans des conditions réalistes pour que soient, si possible, pris en compte tous les besoins, le cercle des ayants-droit (autorités fédérales et cantonales, ainsi que dans certains cas les personnes privées) a tendance à être défini de manière trop large. Si par exemple l'accès à des banques de données, surtout par le biais de procédures d'appel, pouvait être testé durant une phase d'essai, on pourrait mieux définir les besoins lors de l'élaboration d'une loi au sens formel. Toutefois, il ne suffit pas de pouvoir mettre en place et de pouvoir tester uniquement des nouvelles procédures d'appel à des conditions simplifiées; il faut pouvoir procéder dans certains cas à des essais avec des nouveaux systèmes dans leur totalité. Vu la durée assez longue du processus législatif, il faudrait, dans le système actuel, commencer à élaborer une base légale avant que les détails du système d'informatique concerné ne soient connus. En procédant ainsi, le risque serait grand que la base légale ne soit pas en adéquation avec la finalité du système.

L'art. 17*a* contient une clause de délégation qui permet au Conseil fédéral d'autoriser pour une durée maximale de cinq ans le traitement automatisé de données sensibles ou de profils de la personnalité si une phase d'essai est absolument indispensable pour la mise en œuvre technique d'un traitement déterminé. L'art. 17*a* n'assouplit pas de manière générale l'exigence d'une base légale pour le traitement automatisé de données sensibles ou de profils de la personnalité. Il se limite à auto-

39 Voir recommandation 261 du rapport de la Commission de gestion du Conseil des Etats; FF **1999** 5200 et 5226.

riser une «législation expérimentale» dans des situations où la nécessité est réelle. Cette disposition permet ainsi d'examiner et d'évaluer exactement durant une phase d'essai les conséquences que pourrait avoir la réglementation envisagée.

En vertu de l'*al. 1*, le Conseil fédéral a l'obligation de consulter préalablement le Préposé. Le préavis de ce dernier ne lie pas le Conseil fédéral. Pourtant, il est difficilement concevable que le Conseil fédéral, en l'absence de circonstances particulières, passe outre l'avis du Préposé. L'al. 1 prévoit en outre des critères cumulatifs à remplir si le Conseil fédéral envisage d'autoriser un traitement automatisé. Les tâches qui nécessitent ce traitement doivent pour leur part être réglées dans une loi au sens formel (let. a). En outre, des mesures appropriées doivent être prises aux fins de limiter les atteintes à la personnalité (let. b). La let. c prescrit que la mise en œuvre d'un traitement, c'est-à-dire sa mise en place technique ou organisationnelle, doit rendre indispensable une phase d'essai avant la création d'une base légale formelle. Si tel n'est pas le cas, le Conseil fédéral ne peut accorder d'autorisation.

L'*al. 2* énumère les critères qui permettent de déterminer si dans un cas concret une phase d'essai est indispensable. A titre d'exemple, on peut citer des innovations techniques qui sont indispensables à la réalisation technique d'un certain traitement, dont les conséquences ne sont pas encore de prime abord prévisibles (let. a). Tel est notamment le cas lorsqu'un logiciel déterminé n'a pas encore été testé ou utilisé avec des données réelles ou lorsque de nouvelles techniques pour la saisie et la transmission d'informations doivent être introduites (par exemple un système de lecture automatisée des numéros d'immatriculation de véhicules).

En outre, il est possible que l'accomplissement d'une tâche déterminée impliquant un traitement de données nécessite la prise de mesures organisationnelles importantes. Tel est souvent le cas lorsque des organes fédéraux doivent collaborer avec des autorités cantonales (let. b). Ainsi, pour la mise en place d'une banque de données concernant des profils d'ADN[40], les flux d'informations et les rôles des différents acteurs ont dû être définis de manière précise, pour garantir entre autres la meilleure protection possible de la personne concernée.

Enfin, lors de la mise en place de liaisons on-line, une phase d'essai peut s'avérer souvent indispensable pour définir de manière précise le cercle des organismes qui doivent disposer d'un droit d'accès pour l'accomplissement d'une tâche spécifique (let. c). Les droits d'accès peuvent ainsi être optimalisés. Une phase d'essai permet de déterminer si dans un cas particulier la mise en place d'une telle liaison est préférable à une transmission régulière de données telle qu'elle a été pratiquée auparavant.

Selon l'*al. 3*, le Conseil fédéral règle les modalités du traitement dans une ordonnance; la transparence de projets-pilotes est ainsi garantie. Le Conseil fédéral peut en outre fixer dans son ordonnance des mesures tendant à la protection de la personne concernée.

Selon l'*al. 4*, l'organe fédéral responsable a l'obligation de soumettre un rapport d'évaluation au Conseil fédéral dans un délai de deux ans après la mise en œuvre de la phase d'essai. En fonction des conclusions du rapport, il a l'obligation de propo-

40 Voir à ce sujet le message relatif à la loi fédérale du 8 nombre 2000 sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personnes inconnues ou disparues; FF **2001** 19.

ser l'interruption ou la continuation du traitement. Ce rapport pourra également servir de base à l'élaboration d'une loi au sens formel, dans l'hypothèse où l'on propose de continuer le traitement. L'al. 4 souligne le caractère expérimental des phases d'essai rendues possibles en vertu de l'art. 17*a*; de plus, une transparence supplémentaire est créée par rapport à ces projets pilotes.

L'*al. 5* précise sans équivoque possible que le traitement doit être interrompu dans l'hypothèse où la base légale formelle n'est pas entrée en vigueur dans un délai de cinq ans après la mise en place d'un essai pilote; l'existence d'un simple projet ne suffit pas. Il s'agit d'un délai légal qui ne pourra pas être prolongé.

2.19 Art. 18 Collecte de données personnelles

L'al. 2 n'est plus nécessaire puisque la règle selon laquelle la collecte doit être effectuée de manière reconnaissable figure désormais dans la partie générale à l'art. 4, al. 4, et s'applique à toute collecte de données personnelles.

2.20 Art. 19 Communication de données personnelles

Par analogie avec l'art. 17, al. 2, let. c, l'art. 19, al. 1, let. c, du projet tient compte du droit pour la personne concernée de s'opposer au traitement. La let. b a été adaptée à la définition du consentement donnée à l'art. 4, al. 5, du projet.

2.21 Art. 21 Proposition des documents aux Archives fédérales

L'art. 21 tient compte de la nouvelle loi fédérale sur l'archivage du 26 juin 1998 (LAr)[41]. Il reprend, dans la loi, à peu de choses près, la teneur de l'actuel art. 27 OLPD[42].

2.22 Art. 26 Nomination et statut

L'al. 2 tient compte de la situation actuelle puisque le Préposé est déjà rattaché à la Chancellerie fédérale.

L'al. 3 permet au Préposé d'avoir son propre budget comme les autres autorités jouissant d'un statut d'autonomie (p. ex. le Contrôle des finances).

41 RS **152.1**
42 RS **235.11**

2.23 Art. 27 Surveillance des organes fédéraux

En vertu des art. 27 et 29 LPD, le Préposé dispose déjà de compétences d'investigation et d'intervention pour ce qui est du traitement des données par des organes fédéraux ou des personnes privées. Pour la surveillance des organes fédéraux, le droit actuel ne lui permet toutefois pas d'ester en justice[43]. Dans son message du 23 mars 1988[44], le Conseil fédéral avait proposé de donner la possibilité au Préposé, lorsqu'une de ses recommandations n'est pas suivie par un département ou par la Chancellerie fédérale, de porter l'affaire devant la Commission fédérale de la protection des données. Les Chambres fédérales en avaient décidé autrement, préférant laisser aux chefs de département et au chancelier la responsabilité de leurs décisions en la matière. Le Conseil national a encore eu l'occasion de confirmer ce point de vue le 3 mars 1999 lorsqu'il a rejeté une motion von Felten 98.3030 (Droit de recours pour le Préposé)[45].

Il convient cependant de prendre en compte l'évolution du droit européen en la matière. Tant le Protocole additionnel à la Convention STE n° 108[46] que la Directive 95/46/CE exigent que les autorités de contrôle soient dotées du pouvoir d'ester en justice (ou de porter les violations du droit interne à la connaissance de l'autorité judiciaire compétente). Afin de rendre le droit fédéral conforme au droit communautaire et de permettre la ratification du Protocole additionnel, le présent projet prévoit de compléter l'art. 27 LPD par un nouvel al. 6 qui permet au Préposé de recourir contre les décisions des départements et de la Chancellerie fédérale. Il est à noter que le Préposé aura également la faculté de recourir au Tribunal fédéral, en vertu des art. 100, al. 2, let. a, et 103, let. c, OJ[47]. Le Préposé aura ainsi des pouvoirs analogues à ceux qu'il détient dans le secteur privé (art. 29 LPD).

2.24 Art. 29 Etablissement des faits et recommandations dans le secteur privé

La compétence qu'a le Préposé d'établir les faits d'office doit être adaptée aux modifications proposées dans le cadre de la présente révision partielle. L'al. 1, let. b, vise essentiellement la nouvelle obligation d'informer introduite à l'art. 7*a* et autorise le Préposé à établir les faits, s'il y a lieu de craindre une violation de l'obligation d'informer lors d'une collecte de données.

L'al. 1, let. c et d, est modifié et adapté aux modifications concernant l'obligation des personnes privées de déclarer leurs fichiers (art. 11*a*), ainsi que l'obligation d'informer le Préposé dans certains cas de communication transfrontière (art. 6, al. 3).

43 ATF **123** II 542
44 FF **1988** II 421
45 BO **1999** N 115
46 RS **0.235.1**
47 RS **173. 10**

2.25 Art. 31 Autres attributions

La liste des compétences attribuées au Préposé en vertu de l'art. 31 est complétée, respectivement précisée, en relation avec l'art. 6, al. 1 et 3, et avec l'art. 11.

2.26 Art. 34 Dispositions pénales

Les dispositions pénales de l'art. 34 LPD sont complétées par une référence aux art. 7*a* et 7*b* du projet. Elles permettront de sanctionner pénalement les personnes qui fournissent intentionnellement des renseignements inexacts ou incomplets dans le cadre de leur devoir d'information ou qui omettent d'informer la personne concernée lors de la collecte ou lors de décisions individuelles automatisées.

L'al. 2 est adapté à la nouvelle réglementation de l'art. 6.

2.27 Art. 37 Exécution par les cantons

L'art. 37 réalise le second volet de la motion «Liaisons online» et vise à renforcer le niveau de protection des données traitées par les organes cantonaux en exécution du droit fédéral. La motion demande que soient prévues, pour les requêtes et l'installation de liaisons «online» avec les systèmes informatiques de la Confédération, des normes minimales permettant d'améliorer la collaboration entre la Confédération et les cantons. Elle charge en outre la Confédération de régler l'accès, l'utilisation, la protection et le contrôle de ses banques de données[48].

L'art. 37 LPD, dans sa teneur actuelle, contient une norme supplétive, en vertu de laquelle le droit fédéral ne s'applique que si le traitement n'est pas soumis à des dispositions cantonales sur la protection des données, ce qui est encore le cas dans quelques cantons. L'art. 37, al. 1, du projet va plus loin et fixe une norme de protection minimale, tout en maintenant le caractère supplétif de cette disposition. Le droit fédéral s'appliquera désormais, non seulement lorsque le traitement n'est pas régi par des dispositions cantonales de protection des données, mais aussi lorsque ces dispositions cantonales n'offrent pas un niveau de protection adéquat. Par «niveau de protection adéquat», on entend un niveau de protection équivalent à celui de la Convention STE n° 108[49]. Le système prévu à l'art. 37, al. 1, est donc le pendant de celui qui est appliqué aux flux transfrontières. En effet, la Confédération a la responsabilité de s'assurer que les personnes privées et les autorités auxquelles elle communique des données personnelles qu'elle gère respectent les mêmes normes de protection qu'elle. Ainsi que l'a relevé le Conseil fédéral dans sa réponse à la motion «Liaisons online», la sécurité d'un système informatique et la protection des données qui y sont contenues se mesurent à l'aune du maillon le plus faible. Or, le niveau de protection peut différer assez nettement d'un canton à l'autre.

48 Cf. également Rapport de la Commission de gestion du Conseil des Etats; FF **1999** 5200 et 5230.
49 RS **0.235.1**

Lors de la procédure de consultation, la compétence de la Confédération d'adopter la réglementation ici prévue a été mise partiellement en question. On constatera à ce sujet que la Confédération est en principe compétente pour édicter des prescriptions à l'intention des cantons dans le cadre de l'application du droit fédéral, à condition que sa compétence législative ne soit pas limitée à des règles-cadres. De plus, les accords internationaux conclus par la Confédération, en l'espèce la Convention STE n° 108, engagent également les cantons dans leurs propres domaines de compétences.

La Confédération doit ménager autant que possible l'autonomie cantonale, en particulier l'autonomie organisationnelle (art. 46, al. 2, et art. 47 Cst.[50]). Tel est le cas en l'espèce puisque les normes de la LPD ne sont applicables que si les prescriptions cantonales de la protection des données ne garantissent pas un niveau de protection adéquat, soit quand elles ne correspondent pas à la norme de protection de la Convention STE n° 108.

2.28 Dispositions transitoires

Le maître du fichier disposera du délai d'une année dès la date de l'entrée en vigueur de la loi pour prendre les mesures nécessaires en vue d'assurer l'information des personnes concernées visés aux art. 4 al. 4, 7*a* et 7*b*. Il n'est donc pas prévu d'appliquer rétroactivement le devoir d'information de l'art. 7*a* à des données déjà collectées.

3 Conséquences

3.1 Conséquences pour la Confédération

3.1.1 Conséquences pour les finances et pour le personnel

Il est difficile d'estimer avec précision les répercussions des nouvelles exigences liées au devoir d'information de l'art. 7*a* sur les finances de la Confédération et sur l'état du personnel. Elles devraient selon toute vraisemblance être mineures. En effet, si la collecte est effectuée directement auprès de la personne concernée, l'information pourra être donnée sans grand effort supplémentaire (p. ex. au moyen d'une phrase-type insérée dans le document qui sert à la collecte). Si les données sont collectées auprès de tiers, il est fort probable que dans la plupart des cas la collecte ou la communication des données sera prévue expressément par la loi (cf. art. 17, al. 2, LPD), auquel cas on peut renoncer à informer la personne concernée (art. 7*a*, al. 3, *in fine*). Enfin, l'art. 9 du projet prévoit un certain nombre d'exceptions au devoir d'information qui visent spécifiquement le secteur public.

Le Préposé est investi de nouvelles compétences dans une mesure limitée; il ne lui faut donc pas de personnel supplémentaire, du fait de la révision.

50 RS **101**

3.2 Conséquences pour les cantons

3.2.1 Conséquences pour les finances et pour le personnel

La révision ne s'applique aux cantons qu'en marge. Elle aura pour effet indirect d'inciter ceux d'entre eux qui n'auraient pas un niveau de protection adéquat à renforcer leur législation dans le domaine de la protection des données, afin de pouvoir continuer à recevoir les données personnelles qui leur sont communiquées par la Confédération. Il s'agit là toutefois uniquement d'une conséquence indirecte de la révision. Il convient en outre de rappeler que le niveau de protection à atteindre se mesurera à l'aune de la Convention STE n°108, dont les normes sont contraignantes pour les cantons également.

3.2.2 Incidences pour les cantons d'une adhésion au Protocole additionnel à la Convention STE n° 108

Les incidences en droit fédéral de l'adhésion de la Suisse au Protocole additionnel à la Convention STE n° 108 ont déjà été exposées plus haut (cf. ch. 1.2.3.1.2, ainsi que le commentaire des art. 6 et 27). Le projet permet de rendre la LPD conforme à ce Protocole (cf. art. 6 et art. 27, al. 6). De par l'art. 37, al. 1, l'art. 6 s'appliquera également au traitement de données personnelles par des organes cantonaux en exécution du droit fédéral, à moins que les dispositions cantonales de protection des données n'assurent un niveau de protection adéquat. Quant à l'art. 27, al. 6, il s'appliquera par analogie aux organes de contrôle désignés par les cantons lorsque des organes cantonaux traitent des données personnelles en exécution du droit fédéral (art. 37, al. 2, LPD).

Dans les domaines qui ne relèvent pas de l'exécution du droit fédéral et qui ne sont par conséquent pas régis par la LPD, les cantons devront adapter leur législation aux exigences du Protocole additionnel. Cela signifie qu'ils ne devront autoriser le transfert de données à caractère personnel vers un autre Etat ou vers une organisation que si l'Etat ou l'organisation destinataire assure un niveau de protection adéquat. Le droit cantonal pourra prévoir des dérogations pour les intérêts spécifiques de la personne concernée, de même que lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou encore quand des garanties contractuelles suffisantes sont prises. Le Préposé publie déjà une liste indicative des Etats dotés d'une loi sur la protection des données assurant un niveau de protection équivalent au droit suisse, si bien que l'application du Protocole additionnel sur ce point ne devrait pas entraîner de difficultés pratiques insurmontables pour les autorités ni pour les particuliers.

Il incombera aux cantons concernés de prendre les mesures qui s'imposent lorsque le statut et les compétences de leur organe de contrôle ou de leur autorité de surveillance ne respectent pas les exigences du Protocole additionnel. En effet, les autorités chargées de veiller au respect de la protection des données au plan cantonal devront être dotées, elles aussi, de pouvoirs d'investigation et d'intervention, ainsi que du pouvoir d'ester en justice ou de porter des violations aux dispositions de protection des données à la connaissance de l'autorité judiciaire compétente. Une possibilité de recours juridictionnel doit être ouverte contre les décisions des auto-

rités de contrôle. Celles-ci doivent en outre pouvoir être saisies par toute personne d'une demande relative à la protection de ses droits à l'égard des traitements de données personnelles. Les autorités de contrôle doivent exercer leurs fonctions en toute indépendance.

Chaque canton devra examiner la conformité de son droit aux innovations mentionnées ci-dessus.

3.3 Conséquences dans le secteur informatique

L'un des buts du projet est d'amener les maîtres de fichier à davantage de transparence, particulièrement dans le domaine du traitement automatisé des données et d'Internet. Le maître du fichier devra prendre les mesures nécessaires sur le plan informatique pour garantir un traitement des données licite et compatible avec la LPD. Il devra assurer, particulièrement sur Internet, une présentation qui rendra la collecte de données personnelles reconnaissable et qui garantira l'information de la personne concernée lors de la collecte de données sensibles ou de profils de la personnalité. Il devra en outre veiller à la sécurité des données, notamment sur le plan informatique, lorsqu'il délègue le traitement de celles-ci à un tiers. Ces mesures organisationnelles auront pour avantage de faciliter les transactions dans le domaine du commerce électronique et s'inscrivent dès lors dans la perspective d'une utilisation plus judicieuse de l'outil informatique.

La présente révision partielle n'implique que très peu d'adaptations des systèmes informatiques des organes fédéraux. Ces organes doivent déjà rendre la collecte reconnaissable (art. 18 LPD). Ils devront examiner si leur obligation active d'informer lors de la collecte de données sensibles et de profils de la personnalité nécessitera quelques modifications. Indépendamment de la présente révision partielle, le registre des fichiers tenu par le Préposé fait actuellement l'objet d'un remaniement qui le rendra accessible sur Internet (voir commentaire de l'art. 11*a*).

La présente révision partielle aura vraisemblablement des conséquences analogues pour les cantons et les communes.

3.4 Conséquences économiques

Le projet vise à renforcer la transparence dans le domaine de la protection des données en prévoyant notamment un droit à l'information de la personne concernée. Il est en effet de plus en plus difficile pour celle-ci, avec le développement du traitement automatisé des données et d'Internet, de savoir qui collecte des données à son sujet, dans quel but et quels seront les destinataires de cette collecte. Le projet vise également à faciliter les flux transfrontières en garantissant que les données pourront être échangées d'un pays à l'autre. Indirectement, il aura également pour effet de renforcer la confiance des consommateurs envers le traitement de leurs données personnelles, notamment lors de transactions effectuées par voie électronique. De ce point de vue, le projet peut engendrer des retombées positives non seulement pour les consommateurs, mais aussi pour les entreprises qui deviendront ainsi plus attractives, particulièrement dans le domaine du commerce électronique, et par voie de conséquence accroître leur compétitivité. L'importance de la protection des données

pour le commerce électronique a été reconnue par l'OCDE, qui a adopté des directives relatives à la protection des consommateurs et créé un outil de certification des sites Web[51]. Les coûts engendrés par la mise en place des mesures organisationnelles qui permettront d'assurer l'information seront largement compensés par ces retombées positives et l'efficacité du marché s'en trouvera améliorée. La nouvelle réglementation contribuera également à rendre plus attractive la place économique suisse. Elle favorisera les échanges, dès lors que l'existence d'une législation offrant un niveau de protection adéquat correspondant aux normes internationales en matière de protection des données facilitera la libre circulation des données. La signature du Protocole additionnel à la Convention STE n° 108 poursuit le même objectif.

Les principaux bénéficiaires des mesures prévues par le projet, particulièrement au niveau de l'information, seront les consommateurs qui pourront mieux défendre leurs droits et se prémunir d'éventuelles atteintes à leur personnalité. Toutefois, les entreprises privées bénéficieront elles aussi d'avantages dans la mesure où l'introduction de nouvelles tâches liées au devoir d'information sera compensée par des allégements dans le domaine des déclarations. L'intervention de l'Etat sera limitée au strict nécessaire. Le contrôle de la loi dépendra encore plus largement de l'initiative des personnes concernées qui seront mieux informées et auront dès lors la possibilité de défendre leurs droits. Les pouvoirs d'intervention du Préposé dans le secteur privé demeureront sensiblement les mêmes. Une grande autonomie sera laissée aux acteurs économiques qui pourront s'assurer d'un niveau de protection adéquat des données, notamment lors de flux transfrontières par des mesures volontaires telles que la conclusion d'une convention ou l'adoption d'un code de conduite. Des avantages seront également accordés aux entreprises qui pratiquent l'auto-contrôle (conseiller interne, certifications). Le non-respect des dispositions légales sera principalement sanctionné par la voie du procès civil (art. 28 ss CC) et par les recommandations du Préposé.

4 Programme de la législature

Le projet a été annoncé comme «un autre objet» dans le Programme de la législature[52].

5 Bases juridiques

5.1 Constitutionnalité

La nouvelle Constitution fédérale de 1999[53], comme l'ancienne de 1874, ne contient aucune disposition habilitant expressément la Confédération à légiférer. La nouvelle Constitution consacre par contre, à l'art. 13, le droit de toute personne d'être protégée contre l'emploi abusif de données la concernant. Il s'agit là d'un droit fondamental qui n'attribue pas de compétence nouvelle à la Confédération. En vertu de

51 Cf. FF **2001** 817 et 892
52 FF **2000** 2268
53 RS **101**

l'art. 35, al. 2 et 3, Cst., les personnes qui assument des tâches de l'Etat sont tenues de contribuer à la réalisation des droits fondamentaux et les autorités doivent veiller à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, soient aussi réalisés dans les relations qui lient les particuliers entre eux. Dans ce sens, le projet contribue à la réalisation de l'art. 13, al. 2, Cst., tant dans les relations verticales entre autorités et particuliers que dans les relations horizontales entre les personnes privées.

Le projet se fonde sur des compétences dont la Confédération disposait déjà lors de l'adoption de la loi. Dans le domaine du droit privé, le législateur peut s'appuyer sur la compétence de légiférer en matière de droit civil (art. 122 Cst.), de même que sur la compétence de légiférer sur l'exercice des activités économiques lucratives privées (art. 95 Cst) et sur la protection des consommateurs et des consommatrices (art. 97 Cst.). D'autres dispositions constitutionnelles viennent compléter ces normes, comme la compétence de légiférer dans le domaine des assurances privées (art. 98, al. 3, Cst.)[54].

Dans le domaine du droit public, le législateur fédéral s'est appuyé sur le pouvoir d'organisation que lui conférait l'art. 82, ch. 1, aCst. (art. 173, al. 2, Cst.) pour édicter des dispositions de protection des données applicables aux autorités et aux services administratifs. Ainsi que le relevait déjà le Conseil fédéral dans son message du 23 mars 1988 concernant la LPD[55], la Constitution reconnaît aux cantons une pleine autonomie en matière d'organisation et il leur appartient de légiférer sur la protection des données dans leur secteur. 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 le droit fédéral, lequel doit être, il va sans dire, fondé sur une norme constitutionnelle attributive de compétence. Même dans ce cas, la Confédération doit éviter d'empiéter sur les compétences cantonales en matière d'organisation. La Confédération s'est limitée jusqu'ici à édicter des normes de protection des données applicables aux cantons dans les domaines où ceux-ci sont chargés d'exécuter le droit fédéral (cf. en particulier l'art. 37 LPD). Le projet respecte cette limite. Les domaines dans lesquels il étend la protection des données concernent soit le traitement de données par des organes cantonaux en exécution du droit fédéral (art. 37), soit le traitement de données par un organe fédéral conjointement avec des organes cantonaux (art. 16, al. 3).

5.2 Rapport avec le droit international

Le projet est conforme à la Convention STE n° 108 et permet de ratifier le Protocole additionnel du 8 novembre 2001. Il permet également un rapprochement partiel avec le droit communautaire. Au surplus, il y a lieu de se référer au ch. 1.2.3.

54 FF **1988** II 432 ss
55 FF **1988** II 421 ss et 433

5.3 Délégation du droit de légiférer

Le Conseil fédéral est chargé de régler les modalités concernant la nouvelle obligation légale d'informer le Préposé lors de communications de données à l'étranger dans des cas déterminés (art. 6, al. 3, du projet).

Il édictera des prescriptions concernant la reconnaissance de procédures de certification et l'introduction d'un label de qualité en matière de protection des données (art.11, al. 2, du projet).

En outre, il fixera les modalités relatives à la déclaration des fichiers, à la conduite et à la publication du registre des fichiers par le Préposé, ainsi que les autres modalités en rapport avec l'obligation de déclarer (art. 11*a*, al. 6, du projet).

Par une ordonnance, le Conseil fédéral pourra autoriser, à certaines conditions, le traitement automatisé de données sensibles ou de profils de la personnalité dans le cadre de projets pilotes (art. 17*a* du projet).

Table des matières