MESSAGE N° 56 *4 mars 2008*
du Conseil d'Etat au Grand Conseil accompagnant le projet de loi modifiant la loi sur la protection des données (adaptation au droit international, en particulier aux accords Schengen/Dublin)

Nous avons l'honneur de vous soumettre un projet de loi adaptant la loi sur la protection des données aux engagements internationaux (accords Schengen/Dublin et protocole additionnel à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) pris par la Suisse dans le domaine de la protection des données.

Le présent message est structuré de la manière suivante:

1. Engagements internationaux de la Suisse
2. Déroulement des travaux
3. Nécessité de procéder à l'adaptation de la LPrD
4. Lignes directrices et champ d'application du projet
5. Commentaire des articles
6. Répartition des tâches Etat–communes
7. Constitutionnalité et conformité au droit fédéral et européen
8. Conséquences financières et en personnel

1. ENGAGEMENTS INTERNATIONAUX DE LA SUISSE

L'Union européenne et le Conseil de l'Europe ont élaboré des instruments juridiques visant à harmoniser la protection des données au niveau international. Ces instruments définissent un standard minimal de protection qui doit être garanti dans tous les Etats membres. Les principaux sont:

– pour l'Union européenne, la *directive 95/46/CE* du Parlement européen 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;
– pour le Conseil de l'Europe, la convention, du 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (*convention* 108) et son *protocole additionnel*, du 8 novembre 2001, concernant les autorités de contrôle et les flux transfrontières de données.

La Suisse s'est engagée à appliquer le contenu de la directive 95/46/CE, dans l'accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (cf. FF 2004 p. 6090).

Par ailleurs, les Chambres fédérales ont adopté, le 24 mars 2006, l'arrêté fédéral sur l'adhésion de la Suisse au protocole additionnel à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (FF 2006 p. 3521). Ce protocole sera soumis au Conseil fédéral pour ratification et devrait entrer en vigueur le 1er avril 2008.

En conséquence, les règles européennes énoncées dans ces deux actes doivent être transposées dans la législation suisse, y compris au niveau cantonal. Tel est précisément l'objet du projet de révision qui vous est soumis. A signaler que les adaptations de la loi fédérale sur la protection des données (LPD) ont été adoptées le 24 mars 2006, parallèlement à l'adoption du protocole additionnel. Les nouvelles dispositions fédérales sont entrées en vigueur le 1er janvier 2008.

2. DÉROULEMENT DES TRAVAUX

a. <u>En général</u>

Le 15 septembre 2006, la Direction de la sécurité et de la justice a institué un groupe de travail chargé d'élaborer un avant-projet de loi révisant la loi cantonale sur la protection des données accompagné d'un commentaire. La présidence de ce groupe a été confiée à Mme Alexandra Rumo-Jungo, professeure à l'Université, présidente de la Commission cantonale de la protection des données; le groupe était par ailleurs composé de M. Christophe Maillard, conseiller juridique DIAF, de Mme Dominique Nouveau Stoffel, préposée cantonale à la protection des données, de M. Guy Python, préposé à la protection des données de la ville de Fribourg, de M. Thierry Steiert, conseiller scientifique DSJ, de M. Luc Vollery, conseiller juridique SLeg (remplacé dès novembre 2006 par Mme Josette Moullet Auberson, conseillère juridique SLeg) et de Mme Marie-Thérèse Weber-Gobet, députée. Le secrétariat et la tenue du procès-verbal ont été assurés par Mme Lydia Oberson, collaboratrice de l'autorité cantonale de surveillance de la protection des données.

A l'origine, la révision projetée visait un triple but:

– adaptation de la loi cantonale sur la protection des données (LPrD) à la directive 95/46/CE et au protocole additionnel précités;
– adaptation de cette même loi à la récente révision de la LPD;
– prise en compte des expériences faites avec la LPrD depuis son entrée en vigueur.

Il est toutefois rapidement apparu qu'il ne serait pas possible de réaliser les trois volets de cette révision dans les délais impartis par la Confédération pour l'adoption des adaptations des lois cantonales aux accords Schengen/Dublin. Le mandat du groupe de travail a par conséquent été limité au premier volet, à savoir l'adaptation de la LPrD aux exigences du droit international. Les deux autres volets d'adaptations seront réalisés ultérieurement.

b. <u>Soutien de la Conférence des gouvernements cantonaux (CdC) et de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP)</u>

La CdC et la CCDJP sont chargées de la mise en œuvre et du développement des accords Schengen/Dublin en ce qui concerne les cantons. Ces Conférences ont confié à M. Beat Rudin, spécialiste du domaine de la protection des données (ci-après le délégué de la CdC), le soin d'élaborer, à l'intention des cantons, un guide pratique pour la mise en œuvre des prescriptions en matière de protection des données reprises avec les accords Schengen/

Dublin. Ce guide consiste en une liste, complétée par des explications, des exigences générales que doivent remplir les législations cantonales en matière de protection des données dans le cadre de l'association aux accords Schengen/Dublin et de la mise en œuvre des dispositions du protocole additionnel. Ce guide a servi de base aux travaux du groupe chargé de la révision.

c. Procédure de consultation

Du 31 mai au 31 août 2007, le Conseil d'Etat a mis en consultation auprès de ses Directions, des organismes intéressés et des partis politiques le projet du groupe de travail, après y avoir apporté de légères modifications.

Dans l'ensemble, le projet du Conseil d'Etat a été accueilli favorablement. Les réserves les plus nombreuses sont celles liées à la difficulté pour les communes de mettre en place des autorités de surveillance de la protection des données satisfaisant aux exigences imposées par les accords internationaux. Le renforcement des pouvoirs des autorités de surveillance de la protection des données a, pour sa part, donné lieu à deux avis critiques. Pour le surplus, le projet a suscité quelques remarques ponctuelles qui ont été prises en compte dans le projet définitif, lorsqu'elles étaient compatibles avec les exigences du droit international et entraient dans le cadre de la modification en cours, à savoir l'adaptation de la loi actuelle aux engagements internationaux de la Suisse.

3. NÉCESSITÉ DE PROCÉDER À L'ADAPTATION DE LA LPRD

a. En général

L'examen de la LPrD à la lumière du guide pratique précité a montré que la loi actuelle correspond déjà en grande partie aux standards requis.

La forme juridique (loi au sens formel) et les dispositions fixant le champ d'application de la loi, les principes régissant le traitement des données personnelles ainsi que les droits des personnes concernées remplissent en particulier les exigences dictées par les engagements internationaux de la Suisse.

Certaines lacunes ont néanmoins été constatées; elles rendent nécessaires d'adapter la LPrD. Sont visés: l'indépendance de l'autorité de contrôle en matière de protection des données (b.), les pouvoirs de cette autorité (c.) et la réglementation des «flux transfrontières de données» (d.).

Par ailleurs, au cours des travaux, il est apparu qu'il n'est pas toujours aisé de déterminer si la législation actuelle remplit ou non les exigences du droit européen. Les «cas-limites» non retenus dans le projet sont présentés ci-dessous par souci de transparence (e.).

A noter que les exigences de la directive 95/46/CE ainsi que celles de la convention 108 et de son protocole additionnel s'appliquent à l'ensemble de la surveillance de la protection des données, y compris, le cas échéant, à celle assurée par les autorités communales de surveillance et par les autorités instituées par les corporations ecclésiastiques.

b. Indépendance des autorités de contrôle

L'article 28 ch. 1 de la directive 95/46/CE et l'article 1 ch. 3 du protocole additionnel prescrivent que les autorités de contrôle doivent exercer leurs tâches en toute indépendance.

Pratiquement, la garantie de la totale indépendance des autorités de contrôle en matière de protection des données comporte des aspects institutionnels et des aspects personnels (A. Epiney, Datenschutz und «Bilaterale II», Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte, *in* RSJ 2006 121/126 sv.; A. Epiney / S. Theuerkauf, Datenschutz in Europa – Ueberblick und Implikationen in der Bilateralen II, *in* Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, p. 71 ss; B. Rudin / B. Baeriswyl, «Schengen» und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, *in* Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, p. 193 ss).

Sur le plan institutionnel, le mode d'élection de l'autorité de contrôle, son statut au sein de l'organisation cantonale, son autonomie budgétaire ainsi que la liberté dont elle dispose dans la planification et l'exécution de son activité, et la manière dont sont réglées les conditions d'engagement et de résiliation des rapports de travail de la personne qui la dirige sont des éléments-clés.

Les aspects personnels de l'indépendance, quant à eux, supposent que les personnes chargées de la surveillance de la protection des données disposent des qualités personnelles et des compétences requises pour l'exercice de leur tâche et qu'elles ne soient pas soumises à des conflits d'intérêts. Cette dernière condition implique que les personnes concernées soient tenues de faire connaître leurs liens d'intérêts publics ou privés et de se récuser lorsque l'autorité traite de dossiers qui les touchent plus particulièrement.

En pratique, le niveau d'indépendance des autorités de contrôle est fonction de la combinaison de ces divers éléments. Une élection par le parlement et un rattachement à cette autorité offrent naturellement une garantie optimale d'indépendance. Toutefois, le déficit qu'implique par exemple une nomination par l'Exécutif (qui équivaut à la nomination du contrôleur par le contrôlé) peut être compensé par d'autres garanties institutionnelles.

L'organisation actuelle de l'autorité cantonale de surveillance de la protection des données, qui est formée d'une Commission et d'un ou d'une préposé-e, offre déjà de bonnes garanties d'indépendance. En effet, la Commission est élue par le Grand Conseil, auquel doit être adressé le rapport annuel en matière de protection des données. Ce rôle important du parlement permet d'assurer le degré d'indépendance requis, alors que le ou la préposé-e est nommé-e par le Conseil d'Etat. A signaler encore que, sur le plan organisationnel, l'autorité cantonale de surveillance est seulement rattachée administrativement à une Direction du Conseil d'Etat et qu'il n'y donc pas de lien de subordination entre cette autorité d'une part et l'Exécutif et l'administration d'autre part (cf. art. 61 LOCEA).

Cela étant, il apparaît raisonnable de conserver le système actuel en procédant à quelques adaptations dictées par la nécessité de renforcer, conformément aux exigences européennes, l'indépendance de l'autorité cantonale de surveillance de la protection des données. Les adaptations en question sont prévues aux articles 30 et 32 du projet (pour le surplus, cf. ci-dessous commentaires relatifs à ces dispositions).

c. Pouvoirs des autorités de contrôle

L'article 28 ch. 3, 2e et 3e tirets de la directive 95/46/CE et l'article 1 ch. 2a du protocole additionnel prescrivent que les autorités de contrôle en matière de protection des données doivent être dotées de pouvoirs effectifs d'intervention et avoir le pouvoir d'ester en justice dans les cas de violation des dispositions légales sur la protection des données.

– *Pouvoirs effectifs d'intervention*

Selon l'article 28 ch. 3, 2e tiret de la directive 95/46/CE, qui explicite l'article 1 ch. 2a du protocole additionnel, les pouvoirs effectifs d'intervention comprennent notamment le pouvoir «de rendre des avis préalablement à la mise en œuvre des traitements, d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement, ou celui de saisir les parlements nationaux ou d'autres institutions politiques». Ces différentes mesures sont énoncées à titre d'exemples dans la directive. On peut en déduire que la liste n'a pas un caractère cumulatif.

Les législations nationales doivent mettre en place un système garantissant que les mesures requises par les autorités de contrôle en matière de protection des données seront effectivement mises en œuvre. A cet égard, il est précisé, dans les considérants de la directive 95/46/CE, que «en cas de non-respect des droits des personnes concernées par le responsable du traitement des données, un recours juridictionnel doit être prévu par la législation nationale» (cf. cons. 55). Le rapport explicatif sur le protocole additionnel précise pour sa part que les Etats parties «devraient accorder à l'autorité de contrôle le pouvoir, soit d'ester en justice, soit de porter à la connaissance de la justice toute violation aux principes de la protection des données. (…) L'obligation des Parties d'accorder à l'autorité ce pouvoir peut être remplie en lui donnant le pouvoir de prendre des décisions judiciaires» (cf. ch. 15).

Les pouvoirs d'intervention actuels de l'autorité cantonale de surveillance en matière de protection des données ne satisfont pas aux exigences décrites ci-dessus. L'article 30 al. 2 let. c LPrD donne en effet à la Commission cantonale de la protection des données seulement la compétence d'inviter les organes concernés à prendre les mesures nécessaires en cas de violation ou de risque de violation des prescriptions légales. Cette compétence d'adresser des recommandations ne garantit pas que ces violations, ou risques de violations, puissent être prévenus. Les mécanismes ordinaires de contrôle de l'activité administrative ne permettent en effet pas à l'autorité cantonale de surveillance d'imposer le respect des principes de la LPrD si cela va à l'encontre de la volonté des organes concernés, en particulier de celle du Conseil d'Etat. La haute surveillance exercée par le Grand Conseil (cf. art. 189 al. 1 LGC) ne garantit pas l'existence de pouvoirs effectifs d'intervention au sens du droit européen (A. Epiney, Datenschutz und «Bilaterale II», Zu den Auswirkungen der Schengen-Assoziierung auf das schweizerische Datenschutzrecht – ausgewählte Aspekte, *in* RSJ 2006 121/128; A. Epiney / S. Theuerkauf, Datenschutz in Europa – Ueberblick und Implikationen in den Bilateralen II, *in* Datenschutz in Europa und die Schweiz, La protection des données en Europe et la Suisse, p. 75; S. Fürzessery Minelli / S. Brunner, La protection des données et les Accords Schengen/Dublin, in Accords bilatéraux II Suisse–UE et autres accords récents, éd. C. Kaddous / M. Jametti Greiner, p. 438; B. Rudin, Kantonale Datenschutzgesetzgebung: Gesetzpflichtiger Inhalt, expertise du 28 mars 2007 réalisée sur demande du canton de Saint-Gall, p. 47: «Es geht nicht darum, dem Kontrollorgan Entscheidungsbefugnisse einzuräumen, sondern nur darum, die Möglichkeit zu schaffen, dass es erreichen kann, dass die datenschutzrechtlichen Anliegen Eingang in ein förmliches rechtliches Verfahren finden».).

La LPrD doit être adaptée sur ce point (cf. ci-dessous commentaires relatifs à l'art. 22a ainsi qu'à l'art. 27 al. 2).

– *Pouvoir d'ester en justice*

Selon le droit européen, l'autorité de contrôle doit être habilitée à agir en justice en cas de violation des dispositions régissant la protection des données ou à pouvoir porter ces cas à la connaissance de l'autorité judiciaire (art. 28, ch. 3, 3e tiret de la directive 95/46/CE et art. 1 ch. 2a du protocole additionnel).

En dehors des infractions pénales poursuivies d'office, qui peuvent être dénoncées aux autorités de poursuite pénale conformément à l'article 146 al. 2 CPP, l'autorité cantonale de surveillance en matière de protection des données ne dispose pas de cette compétence. Il convient donc de compléter la LPrD dans le sens voulu par la directive européenne. Ce pouvoir d'ester en justice a été intégré dans le présent projet sous forme d'un droit de recours (cf. ci-dessous commentaires relatifs à l'art. 22a ainsi qu'à l'art. 27 al. 2).

d. «Flux transfrontières de données»

Les articles 25 et 26 de la directive 95/46/CE et l'article 2 du protocole additionnel obligent les Etats parties à adopter une réglementation détaillée en matière de «flux transfrontières de données».

La LPrD ne contient pas de règles spécifiques en la matière et doit dès lors être complétée dans ce domaine (cf. ci-dessous commentaire relatif à l'article 12a).

e. «Cas-limites»

Dans les quatre cas suivants, il apparaît préférable, pour les motifs indiqués ci-dessous, de renoncer à insérer de nouvelles dispositions dans la LPrD.

– Devoir d'informer lors de décisions individuelles automatisées

L'article 15 de la directive 95/46/CE prescrit que les Etats doivent adopter des règles spécifiques s'agissant du devoir d'informer lors de décisions individuelles automatisées. Ce devoir doit être compris comme 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 vise à éviter que des décisions soient prises sans appréciation humaine et sans que la personne concernée en soit informée (cf. FF 2003 p. 1945).

La réglementation des décisions de ce type vise toutefois principalement les entreprises privées. Les organes soumis à la LPrD ne sont pas directement concernés.

– *Contrôle préalable*

Selon l'article 20 de la directive 95/46/CE, les Etats membres doivent soumettre à un contrôle préalable les traitements de données susceptibles de présenter des risques particuliers. Il n'est cependant pas nécessaire, dans notre système, de prévoir une disposition sur le contrôle préalable. En effet, le contrôle préalable des actes législatifs, tel qu'il est prévu à l'article 30a al. 1 let. b du projet, qui reprend l'article 30 al. 2 let. b de la loi actuelle, offre une garantie suffisante: le contrôle des traitements effectués par les organes soumis à la LPrD est réalisé dans le cadre du processus législatif. En cas de doute, les organes publics ont naturellement la possibilité de s'adresser au ou à la préposé-e pour s'assurer de la licéité des traitements qu'ils prévoient d'entreprendre.

A signaler que le contrôle préalable n'a pas non plus été introduit dans la LPD.

– *Sanctions*

Selon l'article 24 de la directive 95/46/CE qui reprend l'article 10 de la convention 108, la loi devrait prévoir des sanctions applicables en cas de violation des dispositions sur la protection des données. Ces dispositions ne sont pas reprises dans le projet pour les raisons suivantes.

Les infractions qui constituent une violation du secret de fonction sont déjà sanctionnées en droit actuel (art. 320 CP).

Dans les cas où il n'y a pas violation du secret de fonction, par exemple lorsque des données personnelles sont traitées dans un but autre que celui pour lequel elles ont été collectées ou dans un but qui, selon les règles de la bonne foi, ne peut pas être considéré comme compatible avec celui-ci (cf. art. 5 al. 1 LPrD), le respect des dispositions internationales demanderait en revanche théoriquement que l'on prévoie des sanctions.

En pratique, ces situations pourront cependant à l'avenir être efficacement traitées par l'autorité cantonale de surveillance de la protection des données, grâce aux pouvoirs accrus qui lui sont accordés. Par ailleurs, l'instauration d'un système de sanctions reviendrait à réintroduire, par la petite porte, des éléments relevant du droit disciplinaire, qui a été abandonné en 2003 lors de l'entrée en vigueur de la loi sur le personnel de l'Etat.

Il ne se justifie pas non plus d'introduire un système de sanctions uniquement pour les personnes ou organes qui ne sont pas tenus au secret de fonction, par exemple dans les cas de traitements sur mandat (cf. art. 18 LPrD). En effet, ces personnes ou organes traitent des données sur une base contractuelle impliquant en particulier le respect d'un devoir de discrétion étendu. Le mandataire ne doit pas révéler à des tiers les informations qui lui sont confiées par le mandant; il doit également taire tout ce qu'il apprend ou devine en exerçant son mandat. Il doit également garantir que des tiers ne puissent pas accéder aux données qu'il détient. Par ailleurs, conformément à l'article 18 LPrD, il incombe à l'organe public qui confie des tâches à des tiers de prendre les mesures nécessaires pour écarter les risques de dysfonctionnement et, le cas échéant, y remédier.

– *Extension du droit à l'information*

Le législateur fédéral a introduit dans la LPD une nouvelle disposition régissant l'obligation d'informer lors de la collecte de données personnelles sensibles et de profils de la personnalité (art. 7a nLPD).

Le projet d'adaptation de la LPrD aux exigences du droit international ne contient pas de règle similaire, car, selon le guide pratique du délégué de la CdC, la réglementation de la LPrD actuelle répond déjà aux exigences minimales du droit européen en la matière. L'insertion d'une disposition cantonale étendant le droit à l'information, inspirée du nouvel article 7a LPD, pourra naturellement être étudiée à nouveau dans le prochain volet d'adaptation de la LPrD (cf. ci-dessus ch. 2.a).

4. LIGNES DIRECTRICES ET CHAMP D'APPLICATION DU PROJET

a. Lignes directrices

Les lignes directrices qui ont prévalu lors de l'élaboration du projet sont les suivantes:

– les modifications doivent être limitées à ce qui est nécessaire au vu du droit européen;
– elles doivent transposer les prescriptions européennes de manière à ne pas retarder la mise en application des accords Schengen/Dublin («réussir l'évaluation qui sera réalisée par l'Union européenne»);
– elles doivent s'insérer au mieux dans l'ordre juridique cantonal;
– elles doivent, dans la mesure du possible, ne pas s'écarter des solutions retenues dans la loi fédérale sur la protection des données.

b. Champ d'application

Le champ d'application de ces modifications s'étend à l'ensemble de la protection des données, telle qu'elle est régie par la LPrD. Une limitation de ce champ d'application aux domaines couverts par les accords Schengen/Dublin ne serait pas admissible, ni praticable du reste. En effet, les dispositions du protocole additionnel ont un champ d'application général et ne sont pas limitées au dossier Schengen/Dublin. Par ailleurs, dans le domaine du traitement des données, on ne peut pas «compartimenter» strictement les données dans des catégories étanches. Le standard minimal exigé par l'Union européenne ne peut être garanti que si les exigences de la directive 95/46/CE sont appliquées de manière générale. Finalement, sur le plan interne, il serait difficile de justifier une différence dans la protection accordée par l'Etat selon que les données traitées relèvent du domaine Schengen/Dublin ou non.

5. COMMENTAIRE DES ARTICLES

Remarque préalable

La LPrD actuelle est formulée au masculin. Il est souhaitable de saisir l'occasion de la révision en cours pour adapter les dispositions de cette loi aux exigences de la formulation non sexiste, en application des recommandations applicables en la matière. Seules sont toutefois commentées ci-dessous les modifications ayant une portée matérielle.

Article 12a

La LPrD actuelle ne règle pas expressément les flux transfrontières de données (communications de données à l'étranger).

Conformément à l'article 25 de la directive 95/46 et à l'article 2 du protocole additionnel, les transferts de données personnelles vers des Etats tiers ne doivent en principe être autorisés que si ces Etats offrent un niveau de protection adéquat. Si le niveau de protection requis n'est pas garanti, le transfert doit être interdit sauf dans des cas exceptionnels, à savoir lorsque le droit interne prévoit la possibilité du transfert pour des intérêts spécifiques de la personne concernée ou lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants, ou encore lorsque des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert et sont jugées suffisantes par les autorités compétentes.

Ces dispositions doivent être transposées en droit suisse. Au plan fédéral, un nouvel article 6 a été inséré à cet effet dans la LPD. L'article 12a du projet cantonal reprend matériellement cet article.

L'alinéa 1 énonce le principe selon lequel la communication de données personnelles à l'étranger n'est possible que dans les Etats offrant un niveau de protection adéquat. En principe, l'Etat destinataire offre un tel niveau de protection lorsque sa législation répond aux exigences de la convention 108. Il convient cependant de tenir compte également, dans la mesure du possible, de la manière dont est appliquée la loi étrangère.

L'alinéa 2 énumère les cas exceptionnels dans lesquels une communication est admise, bien que l'Etat destinataire n'offre pas de garanties suffisantes. La formulation des exceptions correspond à celle retenue dans la LPD. Il est ainsi clair que les exceptions prévues par le droit cantonal doivent être interprétées de la même manière que celles qui sont applicables au niveau fédéral. Toutefois, les lettres f) et g) de l'article 6 al. 2 LPD ne sont pas reprises dans le projet cantonal, car elles visent des cas qui n'entrent pas dans le champ d'application de la LPrD.

L'alinéa 3 précise que l'organe public doit informer le ou la préposée cantonal-e à la protection des données de l'existence des garanties prévues à l'alinéa 2 let. a préalablement au transfert des données personnelles.

A noter que le préposé fédéral à la protection des données et à la transparence tiendra une liste des Etats dont la législation offre un niveau de protection adéquat.

Article 22a

L'article 28 ch. 3 2e tiret de la directive 95/46/CE et l'article 1 ch. 2a du protocole additionnel prescrivent que les autorités de contrôle en matière de protection des données doivent être dotées de pouvoirs effectifs d'intervention (cf. ci-dessus ch. 3.c).

Le mécanisme retenu à l'article 22a du projet permet d'ancrer dans la législation cantonale les pouvoirs effectifs d'intervention de l'autorité de surveillance de la protection des données, en restant le plus proche possible de la situation actuelle, qui a fait ses preuves.

Ce mécanisme s'articule de la manière suivante:

Dans un *premier temps*, en cas de violation ou de risque de violation des dispositions sur la protection des données, l'autorité de surveillance de la protection des données formule, comme actuellement, des recommandations (art. 22a al. 1). Elle peut proposer que soient prises toutes les mesures nécessaires au rétablissement ou au maintien d'une situation juridiquement correcte en relation avec le traitement des données personnelles, tel que décrit à l'article 3 let. d LPrD. A titre d'exemples, on peut mentionner l'interdiction de la collecte, l'interdiction de la communication ou la destruction des données.

Le destinataire de la recommandation sera, suivant les cas, l'organe concerné (art. 22a al. 1) ou l'autorité hiérarchique à laquelle il est subordonné (art. 22a al. 2).

Lorsque les violations ou risques de violation sont le fait d'entités hiérarchiquement indépendantes (par exemple la direction d'un établissement ou un conseil communal), l'autorité de surveillance leur transmet directement ses recommandations.

En revanche, lorsque les problèmes sont le fait d'un organe ou d'une personne soumis à un lien de subordination hiérarchique, il convient, dans l'idée de responsabiliser tous les organes concernés, d'informer l'autorité hiérarchique supérieure. Cette autorité exerce en effet une surveillance complète sur ses subordonnés et est ainsi en mesure d'exiger d'eux qu'ils respectent les dispositions applicables en matière de protection des données.

Lorsqu'un organe public fait traiter des données personnelles par un tiers, la situation est similaire à celle qui est réalisée lorsqu'il existe un lien hiérarchique (cf. art. 18). L'organe public dispose, sous l'angle qui intéresse la concrétisation des pouvoirs effectifs d'intervention, de pouvoirs analogues à ceux d'une autorité hiérarchique supérieure. C'est donc à lui que doivent être adressées les recommandations de l'autorité de surveillance.

Dans un *second temps*, le destinataire de la recommandation doit se prononcer, dans le délai imparti par l'autorité de surveillance, sur la suite qu'il entend donner à cette recommandation. Il le fait par voie de décision (art. 22a al. 3).

Cette décision est particulière. En effet, elle ne correspond pas exactement à la notion de décision telle qu'elle est définie à l'article 4 du code de procédure et de juridiction administrative (CPJA): alors que, selon le CPJA, la décision est, pour l'essentiel, une mesure adoptée dans un cas d'espèce en vue de créer, de modifier, d'annuler ou de constater des droits ou des obligations, l'article 22a al. 3 ss du projet vise des «décisions» par lesquelles les destinataires des recommandations expriment simplement leur volonté de suivre, de suivre partiellement ou de ne pas suivre lesdites recommandations.

Les exigences du droit international imposent cependant que l'on introduise dans notre législation ces décisions d'un type particulier (concrétisation des pouvoirs effectifs d'intervention; cf. ci-dessus ch. 3, c, 1er tiret). Les dispositions du CPJA régissant les décisions au sens de l'article 4 de ce code sont applicables par analogie aux décisions prévues à l'article 22a al. 3 du projet.

Dans un *troisième temps*, l'autorité de surveillance de la protection des données a la possibilité d'exiger le respect de sa recommandation en s'adressant à l'autorité ordinaire de recours désignée par le CPJA (al. 4). A défaut d'autorité compétente au sens du CPJA, par exemple lorsque la décision émane d'une Eglise reconnue, le recours doit être adressé au Tribunal cantonal unifié (al. 5).

La procédure spéciale instituée à l'article 22a du projet n'est ouverte qu'aux autorités de surveillance de la protection des données (al. 4 *in fine*). Le projet ne va pas au-delà des exigences du droit international et les particuliers qui pourraient éventuellement être concernés par la violation des règles sur la protection des données doivent, comme c'est le cas actuellement, agir par le biais de l'article 27 LPrD.

Ainsi conçu, ce nouveau mécanisme complète le droit de recours prévu à l'article 27 al. 2 du projet et permet à l'autorité de surveillance de la protection des données d'intervenir efficacement également dans les cas de violations de la loi qui ne lèsent pas directement des personnes concernées au sens des articles 23 à 26 LPrD.

Article 27 al. 2

Cette disposition renforce les pouvoirs de l'autorité de surveillance de la protection des données conformément à l'article 28 ch. 3, 3e tiret de la directive 95/46/CE et à l'article 1 ch. 2a du protocole additionnel, qui exigent que les autorités de contrôles disposent du «pouvoir d'ester en justice» en cas de violation des dispositions applicables en matière de protection des données.

En droit actuel, en dehors des cas d'infractions pénales poursuivies d'office qui peuvent être dénoncées aux autorités de poursuite pénale conformément à l'article 146 al. 2 CPP, seules les personnes dont les droits ou obligations pourraient être atteints par les décisions relatives au traitement de données personnelles ont qualité pour recourir (cf. art. 76 CPJA).

Il convient donc de compléter l'article 27 de la LPrD de manière à étendre la qualité pour recourir à l'autorité de surveillance de la protection des données. Les autorités de recours sont définies aux articles 114 ss CPJA, conformément au renvoi de l'article 27 al. 1 LPrD.

Compte tenu de la volonté de mettre en place un système de contrôle efficace au sens du droit européen, il est nécessaire que l'autorité de surveillance de la protection des données ait connaissance de toutes les décisions susceptibles de recours. A défaut, son contrôle ne pourrait être qu'aléatoire. Le projet prévoit donc que les organes publics communiquent à l'autorité de surveillance de la protection des données les décisions qu'ils prennent en application des articles 23 à 26 LPrD.

Pour le surplus, cf. ci-dessus chiffre 3.c.

Article 29 al. 2 et 3

Ces dispositions fixent les conditions minimales que doivent remplir les autorités communales de surveillance de la protection des données.

On ne saurait se satisfaire d'un niveau de protection inférieur pour la seule raison que les traitements des données personnelles sont surveillés par un organe communal. Dès lors, comme les engagements internationaux pris par la Suisse imposent des exigences strictes en matière d'autorité de contrôle, les autorités communales compétentes doivent remplir ces exigences. Si tel n'est pas le cas, il appartient à l'autorité cantonale de surveillance de veiller au respect de la protection des données par les communes concernées.

Par rapport à la situation actuelle, l'article 29 al. 2 du projet renforce les pouvoirs des autorités communales de surveillance de la protection des données. Elles devront en particulier avoir la qualité pour recourir lorsque les droits d'une personne concernée par un traitement de données sont lésés (cpr art. 27 al. 2 et 30a al. 1 let. d du projet) et être dotées de pouvoirs effectifs d'intervention (cpr art. 22a et 30a al. 1 let. c du projet; cf. également ci-dessus chiffre 3.c).

Par ailleurs, en vertu de l'alinéa 3, les communes devront garantir l'indépendance de leur autorité de surveillance. Cette indépendance comporte un aspect institutionnel, dans le sens où il faut éviter que le surveillant soit soumis d'une manière ou d'une autre à l'influence des personnes et organes qu'il doit contrôler, par exemple en raison de son mode d'élection, de la réglementation de ses rapports de travail, etc. Elle a également une composante financière, dans le sens où l'autorité de surveillance doit être dotée des moyens, financiers et en personnel, nécessaires à l'accomplissement de ses tâches et être libre de disposer comme elle le juge utile du budget qui lui est alloué, à l'instar de l'autorité cantonale de surveillance de la protection des données (sur la notion de l'indépendance, cf. également ci-dessus chiffre 3.b).

A noter que l'article 29 al. 2 de la LPrD actuelle donne déjà la possibilité aux communes d'instituer leur propre autorité de surveillance. Les communes de Bulle, Fribourg, Marly et Villars-sur-Glâne se sont dotées d'une telle autorité. Il incombe à ces communes de veiller à ce que l'organe de surveillance qu'elles ont institué réponde aux exigences du droit européen. Il existe des solutions permettant de réduire les inconvénients du nouveau système. Une piste envisageable pourrait par exemple être celle des regroupements de communes.

Articles 30 à 32

Les dispositions de la LPrD actuelle régissant l'autorité cantonale de surveillance en matière de protection des données ne satisfont pas entièrement aux exigences minimales requises par la directive 95/46/CE et par le protocole additionnel (cf. ci-dessus ch. 3.b et 3.c).

Techniquement, l'insertion des modifications requises dans la LPrD appelle une restructuration formelle des articles 30 à 32. Seules les modifications matérielles sont commentées ci-dessous. Elles concernent les articles 30, 30a al. 1 let. c et d, 31a al. 1 let. f et g, et 32 al. 3 à 6.

a. <u>Article 30</u>

L'article 28 ch. 1 de la directive 95/46/CE et l'article 1 ch. 3 du protocole additionnel prescrivent que les autorités de contrôle doivent exercer leurs tâches en toute indépendance (cf. également ci-dessus ch. 3.b).

L'indépendance institutionnelle de la Commission cantonale de la protection des données est déjà garantie par les règles actuelles de la LPrD (cf. en particulier l'art. 30 al. 1). Le projet reprend par conséquent textuellement cette disposition, en précisant cependant que la durée du mandat du président ou de la présidente et des membres de la Commission est de quatre ans, conformément aux dispositions de la loi réglant la durée des fonctions publiques accessoires. Cette durée correspond à la durée actuelle des mandats.

Toutefois, en pratique, la Commission cantonale de la protection des données ne peut exercer ses tâches de manière vraiment indépendante que si elle dispose des connaissances spécifiques indispensables à une surveillance efficace. A cet égard, le domaine de la santé et

celui de l'informatique sont particulièrement sensibles. Il est par conséquent nécessaire que la Commission bénéficie directement de connaissances particulières dans ces deux domaines. Pour le surplus, elle doit être composée de représentants et de représentantes des domaines les plus concernés par la protection des données. Le choix doit être guidé par les besoins de la Commission et par la disponibilité des personnes disposant des compétences requises pour siéger en son sein (al. 2).

Comme il n'est matériellement pas possible de rassembler toutes les connaissances nécessaires au sein de la Commission, le projet rappelle formellement qu'elle peut s'adjoindre le soutien d'experts ou d'expertes ou faire appel à des tiers (al. 3).

Sur la question de l'indépendance budgétaire, cf. le nouvel article 32 al 3.

b. Article 30a al. 1 let. c

L'article 30a al. 1 let. c renvoie simplement au nouvel article 22a (cf. ci-dessus ch. 3.c et commentaire relatif à l'art. 22a).

c. Article 30a al. 1 let. d

L'article 30a al. 1 let. d renvoie simplement au nouvel article 27 al. 2 (cf. ci-dessus ch. 3.c et commentaire relatif à l'art. 27 al. 2).

d. Article 31 al. 1 let. f et g

Il convient de compléter la liste des attributions du ou de la préposée par deux nouvelles tâches liées au renforcement de la surveillance de la protection des données sur le plan international.

A la lettre f), la collaboration entre les divers organes de contrôle doit être comprise comme un échange d'informations utiles. A signaler que la collaboration est prévue à l'article 28 ch. 6 de la directive 95/46/CE et à l'article 1 ch. 5 du protocole additionnel.

La lettre g) découle quant à elle du nouvel article 12a sur les «flux transfrontières de données».

e. Article 32 al. 3 à 6

L'indépendance totale voulue par le droit européen exige que le statut financier de l'autorité cantonale de surveillance en matière de protection des données soit réaménagé. Cette autorité doit être dotée d'un budget propre, dont elle puisse disposer librement en fonction des besoins liés à l'accomplissement de ses tâches. Cf. références citées ci-dessus ch. 3 b.

En application de ces exigences, l'alinéa 3 de l'article 32 prescrit que l'autorité cantonale de surveillance dispose d'une enveloppe budgétaire.

Les alinéas 4 à 6 correspondent aux exigences posées par le droit européen en matière d'indépendance personnelle des membres des autorités de contrôle pour renforcer la confiance des autorités et de la population à l'égard de ces autorités.

L'alinéa 4 reprend l'alinéa 3 de la LPrD actuelle en le complétant par une adjonction concernant l'obligation de discrétion. Il est ainsi clair que les membres de l'autorité cantonale de surveillance sont soumis à cette obligation, au même titre que les membres des autres commissions de l'Etat (cf. art. 26 du règlement sur l'organisation et le fonctionnement des commissions de l'Etat).

L'alinéa 5 est une nouveauté dans le canton. L'obligation de signaler les liens d'intérêts est cependant déjà connue en droit fédéral et dans d'autres législations cantonales. Les intérêts visés sont par exemple les activités professionnelles, les fonctions assumées au sein de commissions ou au sein d'organes de direction, de surveillance ou de conseil de personnes morales, les fonctions politiques, etc.

L'alinéa 6 est introduit dans le projet pour des motifs de transparence; il explicite simplement un principe déjà applicable en droit actuel.

6. RÉPARTITION DES TÂCHES ETAT–COMMUNES

Théoriquement, le projet n'a pas d'incidence sur la répartition des tâches entre l'Etat et les communes. En pratique, il est toutefois possible qu'il exerce un effet dissuasif sur les communes, en raison des nouvelles exigences à remplir par les autorités de surveillance. Si les communes renonçaient à instituer leurs propres autorités de surveillance, il en résulterait un transfert des tâches correspondantes à l'Etat.

7. CONSTITUTIONNALITÉ ET CONFORMITÉ AU DROIT FÉDÉRAL ET EUROPÉEN

Le projet est conforme à la Constitution cantonale (cf. art. 12 Cst.) et au droit fédéral. Par ailleurs son objectif étant l'adaptation de la législation cantonale aux deux instruments juridiques européens principaux en matière de protection des données (directive 95/46/CE et convention 108, y compris son protocole additionnel), il est également conforme au droit européen.

8. CONSÉQUENCES FINANCIÈRES ET EN PERSONNEL

Le projet de révision, en particulier la mise en œuvre des pouvoirs effectifs d'intervention qui visent à garantir un contrôle efficace au sens de la réglementation européenne, impliquent de nouvelles tâches pour l'autorité cantonale de surveillance:

Conformément à l'article 27 al. 2, cette dernière devra à l'avenir examiner les décisions qui sont communiquées au ou à la préposé-e et déposer les éventuels recours nécessaires à l'encontre de ces décisions.

Elle devra également procéder aux contrôles nécessaires à la mise en œuvre de l'article 22a, ou mandater des tiers à cet effet. A cet égard, elle devra disposer de moyens financiers et en personnel lui permettant d'intervenir activement auprès des organes concernés par la LPrD. Des interventions réactives, faisant suite à des requêtes qui lui seraient adressées, ne sauraient être considérées comme suffisantes au regard des exigences européennes.

Par ailleurs, si elle constate des dysfonctionnements, l'autorité cantonale de surveillance aura, selon le projet, des tâches complémentaires par rapport à la situation actuelle. Elle ne se bornera pas à édicter des recommandations sur les mesures à prendre pour remédier aux problèmes, comme c'est le cas aujourd'hui. Au contraire, si ses recommandations ne sont pas suivies d'effet, elle aura pour tâche de recourir auprès de l'autorité judiciaire

compétente, afin de garantir le respect des dispositions sur la protection des données.

Ces tâches supplémentaires requièrent le renforcement des effectifs en personnel dont dispose le ou la préposé-e à la protection des données. L'augmentation se monte à 0,5 EPT. De plus, les montants alloués pour les travaux de la Commission et pour les contrôles externes devront être augmentés de manière appropriée.

Compte tenu de ces divers éléments, l'enveloppe budgétaire destinée à l'autorité cantonale de surveillance de la protection des données devrait, à l'avenir, se monter à 250 000 francs par année (ce qui correspond à une augmentation de 50 000 francs par rapport à la situation actuelle).

BOTSCHAFT Nr. 56 *4. März 2008*
zum Entwurf des Gesetzes zur Änderung des Gesetzes über den Datenschutz (Anpassung an das internationale Recht, insbesondere an die Abkommen von Schengen und Dublin)

Wir unterbreiten Ihnen einen Gesetzesentwurf zur Anpassung des Gesetzes über den Datenschutz an die einschlägigen internationalen Verpflichtungen der Schweiz (Abkommen von Schengen/Dublin und Zusatzprotokoll zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten).

Diese Botschaft ist wie folgt gegliedert:

1. Internationale Verpflichtungen der Schweiz
2. Ablauf der Arbeiten
3. Notwendigkeit einer Anpassung des DSchG
4. Leitlinien und Geltungsbereich des Gesetzesentwurfs
5. Kommentar zu den einzelnen Artikeln
6. Aufgabenteilung Staat–Gemeinden
7. Verfassungsmässigkeit, Bundesrechtskonformität und Europaverträglichkeit
8. Finanzielle und personelle Auswirkungen

1. INTERNATIONALE VERPFLICHTUNGEN DER SCHWEIZ

Die Europäische Union und der Europarat haben Rechtsinstrumente zur internationalen Harmonisierung des Datenschutzes ausgearbeitet. Diese legen einen Mindestschutz fest, der in allen Mitgliedstaaten gewährleistet sein muss. Die wichtigsten Rechtsinstrumente sind:

– Europäische Union: *Richtlinie 95/46/EG* des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;
– Europarat: Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (*Übereinkommen 108*) und sein *Zusatzprotokoll* vom 8. November 2001 bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung.

Die Schweiz hat sich mit dem Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands verpflichtet, den Inhalt der Richtlinie 95/46/EG anzuwenden (vgl. BBl 2004 S. 6467).

Zudem haben die eidgenössischen Räte am 24. März 2006 den Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten verabschiedet (BBl 2006 S. 3649). Dieses Protokoll wird dem Bundesrat zur Ratifikation unterbreitet und wird voraussichtlich am 1. April 2008 in Kraft treten.

Infolgedessen müssen die Bestimmungen dieser beiden europäischen Rechtsakte in das schweizerische und das kantonale Recht überführt werden. Dies ist der Zweck der vorliegenden Gesetzesvorlage. Es gilt zu beachten, dass die Revision des Bundesgesetzes über den Datenschutz (DSG) am gleichen Tag angenommen wurde wie das Zusatzprotokoll, d.h. am 24. März 2006. Die neuen Bundesbestimmungen sind am 1. Januar 2008 in Kraft getreten.

2. ABLAUF DER ARBEITEN

a. Allgemeines

Am 15. September 2006 setzte die Sicherheits- und Justizdirektion eine Arbeitsgruppe ein, die den Auftrag hatte, einen Gesetzesvorentwurf zur Änderung des kantonalen Datenschutzgesetzes und einen Kommentar dazu auszuarbeiten. Die Arbeitsgruppe wurde von Alexandra Rumo-Jungo, Professorin an der Universität Freiburg und Präsidentin der kantonalen Datenschutzkommission, geleitet und setzte sich wie folgt zusammen: Christophe Maillard, Rechtsberater ILFD, Dominique Nouveau Stoffel, kantonale Datenschutzbeauftragte, Guy Python, Datenschutzbeauftragter der Stadt Freiburg, Thierry Steiert, wissenschaftlicher Berater SJD, Luc Vollery, Rechtsberater GeGA (im November 2006 abgelöst von Josette Moullet Auberson, Rechtsberaterin GeGA), und Grossrätin Marie-Thérèse Weber-Gobet. Das Sekretariat und das Protokoll führte Lydia Oberson, Mitarbeiterin der kantonalen Aufsichtsbehörde für Datenschutz.

Die geplante Revision hatte ursprünglich drei Ziele:

– Anpassung des kantonalen Datenschutzgesetzes (DSchG) an die Richtlinie 95/46 EG und an das oben erwähnte Zusatzprotokoll;
– Anpassung des DSchG an die kürzlich erfolgte Revision des DSG;
– Anpassung des DSchG aufgrund der seit seinem Inkrafttreten gemachten Erfahrungen.

Es zeigte sich jedoch rasch, dass es nicht möglich war, alle drei Ziele innerhalb der Frist zu verwirklichen, die der Bund zur Anpassung der kantonalen Gesetze an die Abkommen von Schengen und Dublin gesetzt hatte. Daher wurde der Auftrag der Arbeitsgruppe auf den ersten Punkt beschränkt, d.h. die Anpassung des DSchG an das internationale Recht. Die beiden anderen Aspekte werden im Rahmen einer späteren Revision behandelt werden.