b) 31. Dezember 2008, für die Bewilligung für Ferienhäuser in Siedlungsgeebieten (Zonen für öffentliche Anlagen).

In Naturschutzgebieten

Der Staatsrat ist der Auffassung, dass ein überwiegendes öffentliches Interesse an der Nichterneuerung der Pachtverträge für Ferienhäuser innerhalb der Naturschutzgebiete besteht. Diese Zonen werden aus Mooren, Schilfbeständen, Wald und anderen natürlichen Vegetationsgebieten gebildet und werden somit direkt durch Bestimmungen des eidgenössischen Rechtes geschützt. Der Erhalt von Bauten in diesen Gebieten ist unvereinbar mit dem langfristigen Erhalt von schützenswerten naturnahen Landschaften und gegen die grundlegenden Ziele der Raumplanung.

In Zonen für öffentliche Bauten

Der Staatsrat vertritt aber die Auffassung, dass eine Überprüfung der Massnahmen betreffend Pachtverträge für Fereinhäuser innerhalb des Siedlungsgebietes (Zonen für öffentliche Anlagen) angestrebt werden muss. Differenziertere Lösungen könnten für eine gewisse Anzahl von Bauten gefunden werden, je nach Einteilung und Nutzung der jeweiligen Zone. Es ist möglich, dass einige Gebäude abgebrochen oder verschoben werden müssen. Andere könnten bestehen bleiben, aber für einen nichtprivaten Gebrauch, oder könnten möglicherweise vom Kanton übernommen werden und einer öffentlichen oder touristischen Nutzung zugeführt werden. Zum jetzigen Zeitpunkt verpflichtet sich der Staatsrat, die verbleibenden 14 Jahre, bis zum Ablauf der Frist, zu nutzen, um eine vertiefte Studie über die Zukunft dieser Ferinhäuser durchzuführen. Informelle Kontakte mit Vertretern der Vereinigung der Eigentümer der Ferienhäuser haben bereits stattgefunden.

Schliesslich wird der Staatsrat, entsprechend dem Vorschlag von mehreren Grossräten während der Debatte über die Erheblicherklärung des Postulates, die Pachtzinse für alle Ferienhäuser, welche auf den Grundstücken des Staates gelegen sind, erhöhen.

SCHLUSSFOLGERUNG

Der Staatsrat ersucht den Grossen Rat, von diesem Bericht Kenntnis zu nehmen.

MESSAGE N° 194
accompagnant le projet de loi sur la protection des données

Fribourg, le 13 septembre 1994

Nous avons l'honneur de vous soumettre un projet de loi sur la protection des données.

Le présent message comprend les chapitres suivants:

I. Introduction
II. Les grandes lignes du projet
III. Commentaire du projet
IV. Conséquences financières

I. INTRODUCTION

1. Le droit de la protection des données a pour but de préserver les libertés et la vie privée des personnes face aux atteintes qui peuvent résulter du traitement de données personnelles.
Cette protection reposait, jusqu'à un passé récent, sur des dispositions ponctuelles du droit civil, du droit pénal et du droit administratif, ainsi que sur la jurisprudence relative aux droits fondamentaux.
Suite au développement de l'informatique et aux nouvelles possibilités de traitement qui en sont résultées, le besoin s'est fait sentir de régler de manière plus systématique et plus spécifique la protection des données personnelles.
C'est ainsi qu'au terme de longs travaux préparatoires, la Confédération a adopté le 19 juin 1992 une loi sur la protection des données (ci-après LPD ou loi fédérale), qui est entrée en vigueur le 1er juillet 1993. Cette loi s'applique, d'une part, à l'administration fédérale, et, d'autre part, à l'ensemble du secteur privé. En revanche, elle ne s'applique en principe pas aux collectivités publiques cantonales et communales.
De leur côté, quatorze cantons ont adopté à ce jour une loi sur la protection des données (Zurich, Berne, Lucerne, Uri, Schwyz, Bâle-Ville, Bâle-Campagne, Thurgovie, Tessin, Vaud, Valais, Neuchâtel, Genève et Jura), et cinq autres un règlement ou des directives. Ces réglementations s'inspirent généralement, comme le présent projet, d'une loi-modèle proposée en 1983 par la Conférence suisse des chefs des départements de justice et police, qui se réfère elle-même à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du 28 janvier 1981 (Convention 108).
2. Donnant suite à une motion du député Dominique de Buman[1], le Conseil d'Etat a chargé en 1989 un expert, le professeur Rainer J. Schweizer, actuel président de la Commission fédérale de la protection des données, d'élaborer, avec le concours d'une commission, un avant-projet de loi sur la protection des données pour notre canton. Déposé à la fin de l'année 1990, cet avant-projet,

[1] Prise en considération le 22 février 1989 (*BGC* 1989, p. 35 ss).

accompagné d'un commentaire circonstancié, a été mis en consultation auprès des partis politiques, des organisations concernées, des communes et des services de l'administration cantonale.
56 organisations et institutions ont répondu à la consultation. A une exception près, elles ont toutes admis la nécessité de légiférer en la matière. Elles ont, d'une manière générale, approuvé les options retenues dans l'avant-projet, tout en demandant un allégement des procédures, un réexamen des moyens prévus pour la mise en œuvre, ainsi qu'une meilleure prise en compte de la situation des communes. En outre, près de 300 observations ou questions ponctuelles ont été formulées.
Par la suite, un groupe de travail restreint a été chargé de retravailler l'avant-projet en fonction des résultats de la consultation. Bénéficiant du concours de M. Jean-Philippe Walter, suppléant du Préposé fédéral à la protection des données, ce groupe a redimensionné l'avant-projet tant sur le plan formel (réduction de 53 à 41 articles) que sur le plan matériel (suppression de procédures d'autorisation ou de préavis; renonciation aux préposés internes; simplification de la déclaration des fichiers), tout en cherchant à en préserver la substance. En outre, il a révisé la systématique et la rédaction de l'avant-projet, dans le but, d'une part, d'harmoniser celui-ci avec la loi adoptée entre-temps sur le plan fédéral, et, d'autre part, de rendre plus compréhensibles des dispositions qui, en raison de leur objet et de leur généralité, demeurent néanmoins souvent très abstraites.

II. LES GRANDES LIGNES DU PROJET

L'essentiel des dispositions du projet constitue un régime de base applicable en principe à tout traitement de données personnelles par des organes publics *(A)*. Comme le projet s'applique également aux communes, il prévoit un certain nombre de dispositions particulières, adaptées à leur situation *(B)*. Enfin, il existe d'autres cas pour lesquels il est nécessaire de prévoir soit des compléments, soit des dérogations aux dispositions générales: traitement de données sensibles, traitement à des fins statistiques, traitement des données de police, etc. *(C)*.

A. RÉGIME DE BASE APPLICABLE À TOUT TRAITEMENT DE DONNÉES

1. Le projet prévoit plusieurs éléments qui se combinent afin d'assurer une protection optimale des données personnelles, ou, plus précisément, des personnes contre les risques liés au traitement de données:
   - il énonce les principes fondamentaux qui doivent régir un tel traitement;
   - il règle la mise en œuvre de ces principes par les administrations publiques;
   - il accorde aux personnes concernées des droits face aux organes de l'administration qui traitent des données;
   - il institue une autorité de surveillance, sous la forme d'une commission et d'un préposé;
   - il instaure, avec la déclaration des fichiers et le registre y relatif, des instruments destinés à jouer un rôle de pivot entre l'administration, les personnes concernées et l'autorité de surveillance.
2. Les principes fondamentaux qui régissent tout traitement de données sont de deux sortes: d'une part, des conditions générales de licéité du traitement, qui spécifient des principes généraux du droit administratif tels que la nécessité d'une base légale ou le respect de la proportionnalité ou de la bonne foi; d'autre part, des règles particulières concernant certaines formes de traitement, telles que la collecte ou la communication de données.
3. La mise en œuvre de ces principes incombe en premier lieu à l'administration: chaque organe est responsable des traitements qu'il effectue, et les supérieurs ont à contrôler l'application de la loi.
   Il y a lieu de relever, en particulier, que lors du développement de systèmes informatiques, les exigences de la protection des données devront être prises en compte dès le début de l'étude.
4. L'effectivité de la protection des données dépend également pour une large part de la possibilité pour la personne concernée de faire valoir des droits, qui sont, pour l'essentiel:
   - le droit d'accéder aux données la concernant;
   - le droit de faire rectifier ou détruire les données inexactes ou illicites;
   - le droit d'obtenir la réparation d'un dommage éventuel dû à un traitement illicite.

   Ces droits permettent aux personnes d'exercer un premier contrôle sur la manière dont l'administration traite les informations qui les concernent, contrôle qui joue également un rôle préventif.
5. Cependant, en pratique, les droits attribués aux citoyens par les législations sur la protection des données ne déploient que des effets limités. C'est pourquoi le projet institue une autorité de surveillance indépendante, dotée d'un pouvoir d'investigation étendu, dont le rôle est double: elle exerce, d'une part, une fonction de contrôle, et, d'autre part, une fonction de conseil. Par contre, le projet renonce à lui attribuer un rôle juridictionnel ou une fonction formelle de médiateur lors de conflits entre l'administration et un citoyen.
6. Enfin, la déclaration de fichier et le registre des fichiers constituent des outils essentiels pour les différents partenaires concernés par la protection des données:
   a) Ils obligent les organes publics à examiner et à régler, préalablement et de manière systématique, les questions qui se posent lors de l'établissement d'un fichier et leur permettent d'avoir une vue d'ensemble sur leurs fichiers.
   b) Ils donnent aux particuliers la possibilité de prendre connaissance de l'existence et des caractéristiques des fichiers tenus par chaque collectivité, et constituent de ce fait un préalable à l'exercice du droit d'accès et des autres droits des personnes concernées.
   c) Ils permettent à l'autorité de surveillance d'exercer sa tâche de contrôle.

B. RÉGIME PARTICULIER APPLICABLE AUX COMMUNES

1. En incluant les communes dans son champ d'application, le projet tend à réaliser une protection des données aussi uniforme que possible dans tout le canton. Malgré le fait que certaines communes sont déjà dotées d'un règlement de protection des données, cette solution, qui n'a pas été remise en cause lors de la procédure de consultation, paraît adéquate: les dispositions matérielles du projet constituent un standard auquel les communes ne pourraient de toute façon pas déroger.
2. Cependant, le projet tient compte, d'une part, de l'autonomie des communes en matière d'organisation administrative, et, d'autre part, des problèmes de praticabilité que la loi peut poser pour les petites communes, notamment pour celles qui ne disposent pas d'une administration permanente.
   Les dispositions suivantes du projet, en particulier, répondent aux spécificités de la protection des données sur le plan communal:
   a) L'article 29 alinéa 2 laisse la faculté aux communes d'instituer leur propre autorité de surveillance, l'autorité cantonale exerçant sa fonction dans les communes qui n'ont pas fait usage de cette possibilité.
   b) L'article 21 alinéa 2 permet aux communes qui n'ont pas leur propre autorité de surveillance de répondre de la manière la plus simple au besoin de leurs habitants de pouvoir se renseigner sur place.
   c) L'article 34 dispense de toute déclaration (et donc de toute tenue de registre) les communes qui n'ont aucun fichier informatisé.

   Par ailleurs, les dispositions existantes de la loi du 23 mai 1986 sur le contrôle des habitants (RSF 114.21.1, ci-après LCH) relatives à la protection des données, soit ses articles 16 à 20, ont été révisées afin de les harmoniser avec le projet, mais aussi pour tenir compte des expériences pratiques faites en la matière (art. 36).

C. SITUATIONS PARTICULIÈRES RÉGIES PAR DES DISPOSITIONS SPÉCIALES

1. Si tout traitement de données personnelles est en soi porteur d'un certain risque pour les droits des individus, la nature des données traitées et la forme du traitement peuvent accroître sensiblement ce risque. Pour faire face à de tels risques accrus, le projet pose des exigences particulières que les organes publics devront respecter lors du traitement de données sensibles (art. 8, art. 19 al. 2 i.f. et art. 20 al. 1), lors d'une communication au moyen d'une procédure d'appel (art. 10 al. 2), lors d'un traitement conjoint (art. 17 al. 2 et art. 19 al. 2 let. e), lors d'un traitement auquel participent des collectivités différentes (art. 19 al. 3), ainsi que lors d'un traitement sur mandat (art. 18 et art. 23 al. 3).
   A l'inverse, il est possible de diminuer la charge administrative qu'engendre pour les organes publics la protection des données lorsque les risques de violation des droits des individus sont particulièrement faibles: ainsi, des exceptions à la déclaration des fichiers sont prévues à l'article 20 et, pour les communes qui ne sont pas encore informatisées, à l'article 34; en outre, l'accès à des données archivées pourra être refusé faute d'un intérêt digne de protection (art. 25 al. 2).
2. Par ailleurs, la nature particulière de certaines tâches publiques exige des règles spécifiques de protection des données, concrétisant les dispositions générales, y dérogeant ou les complétant.
   C'est ainsi que le projet contient des dispositions spéciales:
   - pour le traitement de données personnelles à des fins statistiques ou à d'autres fins ne se rapportant pas à des personnes (art. 14–16);
   - pour le traitement de données personnelles par la police cantonale (art. 39, qui introduit un chapitre sur le traitement des données de police dans la loi du 15 novembre 1990 sur la police cantonale (RSF 551.1, ci-après LPol));
   - pour la communication de données par le contrôle des habitants (art. 35, qui modifie les dispositions y relatives de la LCH).

   Dans les trois cas, les dérogations aux dispositions générales du projet sont contre-balancées par des exigences spécifiques d'ordre matériel ou procédural.
   En ce qui concerne le personnel des collectivités publiques, le projet se limite à insérer dans les lois y relatives une règle de base et un renvoi (art. 36 et 37). Il appartiendra au Conseil d'Etat d'édicter, pour les collaborateurs de l'Etat, une réglementation plus spécifique.
   Dans le domaine de la santé publique, enfin, le projet prévoit une règle spéciale pour l'exercice du droit d'accès (art. 24 al. 3). Pour le reste, les dispositions du projet s'appliquent aussi longtemps qu'elles n'auront pas été spécifiées dans le cadre d'une réglementation sur les droits des patients dans les établissements hospitaliers.

III. COMMENTAIRE DU PROJET

Le présent commentaire ne contient pas un exposé systématique de la matière réglée dans chaque disposition du projet. Il se limite à donner des explications complémentaires qui devraient aider le lecteur à saisir la portée des articles.

Dispositions générales (art. 1–3)

Article premier

1. L'article premier situe le droit de la protection des données dans son contexte, celui de la protection des droits fondamentaux, et plus particulièrement de la liberté personnelle. Il établit ainsi un cadre général pour l'interprétation de la loi.
2. Cette protection des droits fondamentaux s'exerce à l'égard des «organes publics», notion précisée dans la norme consacrée au champ d'application de la loi (art. 2). Les autres termes qui figurent dans cette disposition *(personne concernée, traitement, données personnelles)* sont définis à l'article 3.

Art. 2 al. 1

1. Par «organes» au sens de la lettre a, on entend aussi bien les autorités que les services et, d'une manière générale, les agents des collectivités publiques.
2. Les «autres corporations de droit public» (let. a) sont par exemple les associations de communes, les syndicats d'amélioration foncière, les caisses locales d'assurance du bétail.
3. Sont des «établissements de droit public» (let. a) aussi bien des institutions dotées de la personnalité juridique (Université, Institut agricole de Grangeneuve, Etablissement cantonal d'assurance des bâtiments, Etablissements pénitentiaires de Bellechasse, hôpitaux cantonaux, Office cantonal des assurances sociales) que des institutions sans personnalité juridique (collèges cantonaux, institutions culturelles de l'Etat), ainsi que les fondations de droit public.
4. L'article 2 alinéa 1 let. b reprend la formule utilisée à l'article 2 let. d du code du 23 mai 1991 de procédure et de juridiction administrative (RSF 150.1, CPJA). Les particuliers qui accomplissent des tâches de droit public sont par exemple les notaires, ou les médecins et aumôniers de prisons. Parmi les institutions visées, on peut citer l'Union fribourgeoise du tourisme, ou la Société des cafetiers, restaurateurs et hôteliers s'agissant de la formation des futurs exploitants.

Art. 2 al. 2

1. Cette disposition définit les situations dans lesquelles certains des organes mentionnés à l'alinéa 1 échappent au champ d'application de la loi.
2. L'exception dont jouit le pouvoir législatif (let. a), limitée aux délibérations, s'exprime notamment par le fait que le droit d'accès ne peut être invoqué à l'égard des procès-verbaux non publiés, et que la rectification des propos tenus lors des délibérations ne peut être exigée.
   Sur le plan cantonal, les commissions pour lesquelles la portée de l'exception est la plus grande sont les commissions de naturalisation et de recours en grâce.
3. Les procédures en cours sont soumises, dans les lois qui les régissent, à des prescriptions relativement détaillées visant à protéger la personnalité des individus. C'est le cas notamment des dispositions sur le droit d'être entendu, le droit d'accéder aux dossiers. Si l'on veut éviter que deux législations visant partiellement le même but se superposent, il faut donc exclure ces procédures du champ d'application du projet (let. b).
   Deux exceptions à cette exclusion sont cependant nécessaires:
   a) Dans ses activités de police judiciaire, qui relèvent de la procédure pénale, la police reste soumise à la loi sur la protection des données, pour autant que les règles de la procédure pénale ne s'y opposent pas (art. 38a al. 3 LPol, introduit par l'art. 39). Cette différence de régime entre la police et les autres organes de poursuite pénale tient notamment au fait que les autorités judiciaires ne traitent les données que pour les besoins de la procédure en cours, alors que la police peut à certaines conditions conserver en vue d'une réutilisation ultérieure les données qu'elle recueille dans une procédure.

   b) Parmi les procédures administratives, seules sont mentionnées à l'article 2 alinéa 2 let. b les procédures de juridiction administrative. Cela signifie que la loi s'applique aux procédures administratives de première instance, comme c'est le cas sur le plan fédéral.

   Par ailleurs, il est entendu que les organes judiciaires sont soumis aux dispositions du projet lorsqu'ils traitent des données en dehors d'une procédure en cours.
4. Contrairement à la solution retenue sur le plan fédéral (art. 23 al. 1 LPD), les organes cantonaux et communaux qui agissent selon le droit privé restent soumis aux dispositions de protection des données applicables aux organes publics. Seule exception à ce principe: lorsqu'elles agissent en situation de concurrence économique, les entreprises publiques telles que les Entreprises électriques fribourgeoises, la Banque de l'Etat de Fribourg ou la Compagnie des chemins de fer fribourgeois sont soumises au régime prévu par la loi fédérale pour les entreprises privées.

Art. 2 al. 3

Les paroisses et autres corporations ecclésiastiques des Eglises reconnues sont des corporations de droit public, et sont donc en tant que telles soumises au projet. Afin de tenir compte de leur autonomie, consacrée par la loi du 26 septembre 1990 concernant les rapports entre les Eglises et l'Etat (RSF 190.1, ci-après LEE), le projet réserve toutefois la possibilité pour les Eglises reconnues d'adopter leurs propres dispositions en la matière. Le cas échéant, celles-ci devront au moins prévoir les éléments essentiels de la protection des données, tels qu'ils sont admis par la jurisprudence même en l'absence de législation.

Si une Eglise reconnue devait choisir cette solution, le droit cantonal de la protection des données n'aurait plus de portée propre pour elle, sauf en ce qui concerne la communication de données personnelles par l'Etat et les communes, dans le cadre de l'entraide administrative due par ces derniers (voir art. 37 i.f., 38 et 40).

Art. 3

1. Les définitions contenues dans cet article sont reprises textuellement de la législation fédérale, notamment de l'article 3 LPD.
2. «Données personnelles» (let. a): le projet, comme d'ailleurs la loi fédérale, part de l'idée que toutes les données personnelles sont dignes de protection. Ce sont en premier lieu le but et le contexte dans lesquels une information est utilisée qui déterminent le besoin de protection: une donnée qui paraît anodine à première vue peut se révéler extrêmement délicate dans des situations particulières. Encore faut-il que les données se réfèrent à une personne qui soit au moins identifiable, c'est-à-dire dont l'identification est possible sans le recours à des moyens disproportionnés.
3. «Personne concernée» (let. b): conformément aux règles relatives à la protection de la personnalité posées par le droit civil, le projet attribue les mêmes droits aux personnes morales qu'aux personnes physiques; cette solution est d'ailleurs celle de la loi fédérale.

4. «Données sensibles» (let. c): le besoin de protection d'une donnée dépend en premier lieu du contexte et du but dans lesquels cette donnée est utilisée. Il est cependant certaines données, énumérées de façon exhaustive à l'article 3 let. c, qui peuvent être considérées – à l'instar de ce que prévoit le droit fédéral – comme sensibles par nature. Elles exigent dès lors dans tous les cas des mesures de protection particulières: devoir de diligence accru (art. 8), justification de la nécessité de les traiter (art. 19 al. 2 i.f.), obligation générale de déclarer les fichiers contenant de telles données (art. 20 al. 1).
Contrairement à ce qui est prévu dans la loi fédérale, il n'a pas paru nécessaire de définir dans le projet la notion de «profil de la personnalité»: aucune disposition n'est rattachée à cette notion qui, dans la pratique, est sujette à des interprétations contradictoires.

5. «Traitement» (let. d) et «communication» (let. e): le champ d'application matériel du projet recouvre non seulement les traitements automatisés mais aussi les traitements manuels, ainsi que les formes mixtes. L'opportunité de définir la communication, qui est une forme de traitement, repose sur le fait que celle-ci comporte des risques particuliers, ce qui explique les dispositions détaillées que la loi comporte à son sujet (art. 10–12, art. 15 al. 2, art. 19 al. 2 let. f, art. 26 al. 2 let. a, ainsi que les dispositions de la LCH et de la LPol introduites par les art. 35 et 39).

6. «Fichier» (let. f): cette notion recouvre aussi bien le fichier proprement dit que les dossiers auxquels ce fichier permet d'accéder. Deux instruments essentiels de la protection des données y sont directement rattachés: d'une part, la déclaration des fichiers et le registre y relatif (art. 19 ss), et, d'autre part, le droit d'accès (art. 23 ss).

7. «Responsable du fichier» (let. g): le responsable du fichier joue un rôle essentiel en ce qui concerne la déclaration du fichier (art. 19 al. 1 et 3) et l'octroi du droit d'accès (art. 23 et 25). Il doit être distingué de l'organe qui, traitant des données à n'importe quel niveau hiérarchique, est responsable du respect des dispositions de protection des données pour les traitements qu'il effectue (art. 17 al. 1): les deux notions peuvent coïncider, elles sont néanmoins différentes.

8. «Participant au fichier» (let. h): la définition du statut de participant, auquel sont rattachées plusieurs dispositions du chapitre consacré à la mise en œuvre de la protection des données (art. 17 al. 2, art. 19 al. 2 let. e et al. 3 et art. 21 al. 2), est reprise des articles 3 alinéa 1 let. g et 16 alinéa 1 let. g de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD). A la différence d'un destinataire des données, qui reçoit une simple communication et n'a donc pas la possibilité de traiter activement les données dans le fichier d'origine, le participant est en droit d'agir directement sur tout ou partie du contenu du fichier, sans toutefois avoir le statut de responsable du fichier.
L'on peut donner, comme exemples de participants à un fichier dans l'administration cantonale, le Bureau de la taxe militaire, pour le fichier «Gestion des adresses des contribuables», tenu par le Service cantonal des contributions, et les registres fonciers des districts, pour la base de données «Descriptif cadastral», tenue par le Service du cadastre.

Conditions générales de licéité du traitement (art. 4–8)

Art. 4

1. Le traitement des données personnelles par des organes publics est une activité administrative soumise au principe de la légalité: seule une base légale permet à un organe public de traiter des données qui, à l'origine, appartiennent à la personne.

2. La question de savoir quel degré de précision doit avoir la disposition légale, et à quel niveau elle doit se situer, est régie par les principes généraux du droit constitutionnel et du droit administratif. Elle sera résolue en tenant compte de l'importance des risques d'atteinte aux droits des personnes que représente le traitement prévu.
L'article 10 alinéa 2, en exigeant une base légale spécifique pour l'accès à des données personnelles au moyen d'une procédure d'appel, constitue une concrétisation de ce principe.

Art. 5

1. Le principe de finalité émane du principe de la bonne foi: lorsqu'elle fournit des informations sur son compte, la personne ne le fait pas inconditionnellement, mais en vue d'un traitement déterminé; une réutilisation de ces informations à des fins différentes peut dès lors être contraire aux règles de la bonne foi.

2. Tel qu'il est énoncé à l'alinéa 1, le principe de finalité présente deux volets:
   a) D'une part, toute collecte de données doit s'effectuer dans un but déterminé; la détermination de cette finalité préalable au traitement exclut que des données soient collectées de manière illimitée, en prévision de buts insuffisamment définis.
   b) D'autre part, les données collectées dans un but déterminé ne peuvent pas être traitées ultérieurement dans un but incompatible avec la finalité initiale.

3. Le but du traitement résulte de la tâche de l'organe (et donc de la base légale), et c'est en fonction de ce but que s'apprécient la nécessité et la pertinence des traitements (art. 6) ainsi que l'exactitude des données (art. 7).

4. Le principe de finalité se rapporte au droit de la personne à maîtriser les informations la concernant. Dès lors, la personne concernée peut renoncer à ce droit en consentant à une utilisation de ces données à de nouvelles fins (al. 2). Cette possibilité présentera un intérêt principalement en matière de communication, où elle permettra par exemple d'éviter la collecte répétée de données identiques, qui pourrait être perçue par les personnes concernées comme une tracasserie administrative.

5. Le principe de finalité est atténué en matière de communication de données en vue d'un traitement à des fins ne se rapportant pas à des personnes (art. 15 al. 2 let. b).
Par ailleurs, la loi établit dans deux cas une présomption de compatibilité des buts: à l'article 15 alinéa 1 (traitement à des fins ne se rapportant pas à des personnes), ainsi qu'à l'article 38d alinéa 1 LPol introduit par l'article 39 (conservation de données de police en vue de leur réutilisation).

6. Sur les relations entre entraide administrative et principe de finalité, cf. infra N° 2 ad article 10.

Art. 6

Le respect du principe de proportionnalité lors de chaque étape du traitement est l'un des éléments essentiels de la protection des données: il s'impose depuis la phase de la collecte – les données devant être adéquates, pertinentes et non excessives par rapport au but visé – jusqu'à la phase de la destruction ou de l'archivage, en passant par l'exploitation et la communication des données.

Art. 7

1. L'exactitude dont il est question dans cette disposition est une exactitude relative: les données doivent être conformes à l'état d'information dans lequel se trouve l'administration au moment du dernier traitement – état d'information qui correspondra d'ailleurs dans la plupart des cas aux renseignements fournis par la personne elle-même (principe de la collecte auprès de la personne concernée, art. 9 al. 1) –, et une obligation de vérification n'incombe à l'organe public que dans la mesure où elle est imposée par les besoins de sa tâche.
2. La nécessité de réactualiser les données avant chaque utilisation découle du principe d'exactitude. L'étendue de la mise à jour qui doit être effectuée par l'organe public dépend, comme l'exactitude des données, du but du traitement. L'exactitude et la mise à jour des données prennent une importance toute particulière lors de la communication de données.
3. Sur le droit de rectification des données inexactes, cf. article 26 alinéa 2.

Art. 8

La concrétisation du devoir de diligence accru imposé par cette disposition incombe aux organes de l'administration, qui doivent prendre les mesures adéquates pour faire face aux risques particuliers engendrés par le traitement de données sensibles.

Dans la pratique, ce devoir de diligence se traduira notamment par une certaine circonspection lors de la collecte et de la communication de données sensibles, ainsi que par l'adoption de mesures particulières de sécurité au sens de l'article 22.

Conditions supplémentaires applicables à certaines formes de traitement (art. 9–13)

1. L'édiction de ces dispositions est justifiée par le fait que les risques d'atteinte aux droits des personnes sont particulièrement élevés à deux moments-clés du traitement: l'entrée et la sortie des données.
2. Comme le titre de la section l'indique, il s'agit de conditions supplémentaires: les conditions générales posées aux articles 4 à 8 s'appliquent donc également à ces formes particulières de traitement.

Art. 9

1. Le terme «collecte» désigne toute forme d'obtention des données, et recouvre l'obtention auprès d'un organe public (ce dernier effectuant, de son point de vue, une communication de données).

2. Le principe de la collecte auprès de la personne concernée (al. 1) et le droit d'être renseigné sur le traitement (al. 3) découlent de la maîtrise de la personne sur les informations la concernant, alors que le principe de la collecte reconnaissable (al. 2) repose sur le respect de la bonne foi.
3. La collecte auprès de la personne concernée est la règle, mais il ne s'agit pas d'un principe absolu (al. 1 deuxième phrase).
   Un exemple de «disposition légale» prévoyant la collecte auprès d'un tiers figure à l'article 14 (collecte auprès d'un organe public en vue d'un traitement à des fins ne se rapportant pas à des personnes).
   La «nature de la tâche», quant à elle, vise notamment les tâches de la police, dont l'accomplissement exige souvent une dérogation au principe de la collecte auprès de la personne concernée.
   Enfin, les «circonstances particulières» permettent une telle dérogation par exemple lorsque la personne concernée n'est pas en mesure de fournir elle-même les données.
4. Lorsque la collecte ne peut avoir lieu auprès de la personne concernée, elle s'effectue si possible auprès d'un organe public, ou, à défaut, auprès d'une tierce personne privée.
   L'organe qui effectue la collecte doit alors avoir particulièrement à l'esprit la nécessité de traiter des données exactes au sens de l'article 7, ce qui comporte pour lui, dans la mesure où le but du traitement l'exige, une obligation de vérification.
5. L'alinéa 3 répond à une exigence de transparence généralement reconnue.

Art. 10 à 12

1. Les dispositions des articles 10 à 12 traitent de la communication de données. Communiquer des données, c'est les rendre accessibles à un tiers. Cette notion recouvre donc aussi bien la communication dans un cas d'espèce que la communication régulière, la transmission de renseignements que l'autorisation de consulter, ou encore la publication.
   La procédure d'appel mentionnée à l'article 10 alinéa 2 constitue une forme particulière de communication régulière, sous forme d'une autorisation générale d'accéder aux données (cf. infra N° 4 ad art. 10).
2. Les articles 10 à 12 ne visent pas les communications exigées par l'accomplissement de la tâche de l'organe qui communique. Ces communications sont néanmoins soumises aux conditions générales des articles 4 à 8.
3. Les dispositions des articles 10 à 12 s'appliquent aussi bien à la communication de données à des organes publics qu'à la communication de données à des personnes privées.
   La communication à des organes publics vise non seulement les organes définis à l'article 2 alinéa 1, mais également les organes de la Confédération, des autres cantons et de leurs communes.
   Quant à la communication à des personnes privées, elle constitue l'exception. Une telle communication se fera d'ordinaire par le préposé au contrôle des habitants, soumis à des dispositions spéciales (réserve de l'art. 12).

Art. 10

1. L'article 10 ne constitue pas une habilitation à communiquer; il se limite à soumettre les différentes formes de communication à des conditions minimales, qui s'ajoutent aux conditions générales des articles 5 à 8:
   a) La communication dans un cas d'espèce doit, soit être prévue par une disposition légale (al. 1 phrase introductive), soit remplir l'une des conditions posées aux lettres a à c de l'alinéa 1.
   b) La communication régulière de données doit être expressément prévue par une disposition légale (al. 1 phrase introductive).
   c) L'octroi d'un accès par procédure d'appel doit également être prévu en tant que tel dans une disposition légale (al. 2).
2. Lorsqu'une disposition légale prévoit expressément la communication régulière ou dans un cas d'espèce (par exemple, art. 40 al. 2 de la loi du 20 septembre 1967 sur le notariat, RSF 261.1), la question du respect du principe de finalité, qui se pose lors de chaque communication, a été tranchée par le législateur; de ce fait, l'organe qui communique les données est dispensé de s'interroger sur l'application de ce principe.
   L'article 50 CPJA pose à cet égard un problème particulier. Il impose aux autorités administratives la communication de documents, renseignements et rapports lorsque ceux-ci sont nécessaires à l'établissement des faits. En dépit de son caractère général, cet article doit être considéré comme une disposition légale au sens de l'article 10 alinéa 1 du projet, du moins lorsqu'il est invoqué dans le cadre du champ d'application formel du CPJA, c'est-à-dire dans le cadre d'une procédure tendant à la prise d'une décision au sens de l'article 4 CPJA. Il faut cependant relever que le principe de finalité pourra néanmoins être pris en considération par l'organe qui communique les données, comme l'un des éléments de la pesée des intérêts qu'il est appelé à effectuer en vertu de l'article 50 alinéa 2 CPJA (notamment au titre de l'intérêt privé mentionné à la let. b).
3. Lorsqu'aucune disposition légale ne prévoit la communication, celle-ci ne peut avoir lieu que dans un cas d'espèce.
   L'alinéa 1 let. a consacre le principe de l'entraide administrative en dehors des procédures administratives de première instance (la communication de données dans le cadre de telles procédures étant réglée par l'art. 50 CPJA). Cette entraide est régie par les principes de proportionnalité et de subsidiarité.
   L'alinéa 1 let. b établit une pondération des intérêts lors d'une communication à une personne privée. Cette disposition peut autoriser une communication même dans des cas dans lesquels la personne concernée s'y est opposée.
   Le consentement de la personne concernée à ce que la communication ait lieu (art. 10 al. 1 let. c) – qui ne comporte pas nécessairement un consentement à un changement de finalité au sens de l'article 5 alinéa 2 – permet la communication aussi bien à des personnes privées qu'à des organes publics.
4. La procédure d'appel mentionnée à l'alinéa 2 est un mode d'accès automatisé par lequel le destinataire des données, en vertu d'une autorisation du responsable du fichier, décide de son propre chef, sans contrôle préalable (principe du libre-service), du moment et de l'étendue de la communication (dans les limites de l'autorisation). Dans un tel cas, c'est l'impossibilité pour l'organe communiquant de vérifier de cas en cas si les principes généraux de protection des données sont respectés qui fonde la nécessité d'une base légale autorisant expressément une telle procédure.

Art. 11

1. La licéité d'une communication doit être établie non seulement par rapport aux conditions de l'article 10 et aux conditions générales; elle dépend également de l'absence de restrictions à la communication au sens de l'article 11, disposition qui correspond pour l'essentiel à l'article 19 alinéa 4 LPD.
   La lettre a exige dans tous les cas une pondération des intérêts en présence, qui peut d'ailleurs se recouper avec celle qui est prévue à l'article 10 alinéa 1 let. b.
   La lettre b constitue une simple réserve déclaratoire, qui concerne les obligations spéciales de garder le secret (secret médical, par exemple).
2. Lorsqu'une personne fait valoir un intérêt digne de protection à ce que des données la concernant ne soient pas communiquées, l'organe auquel elle s'est adressée devra en tenir compte lors de la pesée des intérêts imposée par la lettre a. Dès lors, il n'est pas nécessaire de prévoir un droit de blocage général dans le projet, ce d'autant moins que celui-ci, contrairement à l'article 19 alinéa 2 LPD, n'autorise pas une communication libre de certaines données. Par ailleurs, la possibilité d'un blocage présente un intérêt surtout en ce qui concerne la communication à des personnes privées, qui relève principalement du contrôle des habitants (cf. art. 18 LCH, modifié par l'art. 35).

Art. 13

1. L'obligation de détruire les données dès que l'organe n'en a plus besoin (al. 1) découle directement du principe de proportionnalité (art. 6).
2. La destruction physique des données est la règle. Néanmoins, elle peut être remplacée dans certains cas par l'anonymisation, dans la mesure où celle-ci est suffisante pour éviter une repersonnalisation des données. L'anonymisation est utile surtout en vue d'une utilisation des données à des fins statistiques, de recherche ou de planification (cf. art. 16 al. 1).
3. Le besoin défini à l'alinéa 1 est celui de l'organe responsable du traitement; ce besoin recouvre diverses finalités, mais il s'agit toujours d'un besoin à des fins d'administration active, qui n'inclut pas la conservation en vue de l'archivage.
4. Cette optique justifie que l'on réserve les dispositions sur les archives (al. 2), qui se situent sur un autre plan que la législation relative à la protection des données. La réserve renvoie aux articles 19 et suivants de la loi du 2 octobre 1991 sur les institutions culturelles de l'Etat (RSF 481.0.1) et à l'article 103 de la loi du 25 septembre 1980 sur les communes (RSF 140.1, ci-après LCo), ainsi qu'à leurs dispositions d'application: règlement du 2 mars 1993 concernant les Archives de l'Etat (RSF 481.1.11), et article 64 du règlement du 28 décembre 1981 d'exécution de la loi sur les communes (RSF 140.11). Elle concerne non seulement le versement aux Archives, mais aussi la conservation et le préarchivage des documents par l'organe public avant que celui-ci ne s'en dessaisisse.

Bien que les dispositions sur les archives imposent comme règle la conservation des documents détenus par les organes publics (cf. art. 9 du règlement concernant les Archives de l'Etat), il n'y a pas contradiction entre le principe posé à l'article 13 alinéa 1 et cette conservation. La destruction intervient en effet à trois stades de la vie des données: destruction au jour le jour des documents surnuméraires, épuration lors du préarchivage, et destruction de certains documents lors du versement aux archives. En fin de compte, l'archivage ne concerne qu'un faible pourcentage de l'ensemble des documents établis par l'administration.

5. La protection des données personnelles qui sont archivées doit être réglée de façon spécifique dans la législation concernant l'archivage; les dispositions relatives aux délais de consultation (délais à l'expiration desquels les documents des archives sont accessibles au public) en constituent un premier élément.
   Le projet ne règle en la matière que le droit d'accès des personnes concernées et les droits de ces personnes en cas d'atteinte (art. 25 al. 2 et art. 26 al. 3).

Traitement de données à des fins ne se rapportant pas à des personnes (art. 14–16)

1. La réglementation spéciale prévue pour le traitement à des fins ne se rapportant pas à des personnes se justifie du fait que ce genre de traitement crée moins de risques pour les droits des individus, dans la mesure précisément où il ne se rapporte pas à des personnes et où certaines prescriptions spécifiques sont respectées. Par ailleurs, ces dispositions tiennent compte de l'intérêt public que présentent la recherche scientifique, la planification et la statistique.
2. L'article 14 cite comme exemple d'un tel traitement la recherche. Cependant, lorsqu'elle comporte le traitement de données personnelles en tant que telles, la recherche scientifique ne bénéficie pas de ces règles particulières; en l'absence d'une législation traitant spécifiquement de la question, elle demeure donc soumise aux règles habituelles.

Art. 14

L'article 14 pose une dérogation au principe de la collecte auprès de la personne concernée (art. 9 al. 1). Lorsque, par exemple, il s'agit de se procurer, pour des travaux statistiques, des données qui existent déjà auprès d'un autre service, l'organe public évitera, en vertu du principe de proportionnalité, de solliciter sans nécessité les personnes concernées.

Art. 15

1. L'article 15 alinéa 1 constitue une base légale pour le traitement des données personnelles à des fins de statistiques, de recherche ou de planification. La dérogation au principe de finalité qui est contenue dans cette base légale est atténuée par le fait que le traitement doit intervenir «dans l'accomplissement de la tâche de l'organe», formule qui conserve l'idée d'une certaine compatibilité des buts.
2. Par traitement au sens de cette disposition, il faut entendre notamment la conservation et l'exploitation des données, ainsi que la publication des résultats du traitement. Par contre, la collecte est exclue par le fait que les données doivent déjà être en possession de l'organe («qui les détient»), et la communication est traitée de façon spécifique à l'alinéa 2.
3. L'article 15 alinéa 2 constitue une base légale pour la communication à un organe public. Si cette base légale est suffisante aussi bien pour une communication dans un cas d'espèce que pour une communication régulière, elle ne permet pas l'octroi d'un accès au moyen d'une procédure d'appel (cf. art. 10 al. 3).
   La lettre a reprend, en l'atténuant, le principe posé à l'article 10 alinéa 1 let. a. Elle concerne notamment les communications aux services (cantonal ou communaux) de statistique.
   Quant à la lettre b, elle assouplit le principe de finalité, sans qu'il y ait toutefois exemption complète du respect de la compatibilité des buts.

Art. 16

L'article 16 pose, en matière de traitement à des fins ne se référant pas à des personnes, des conditions particulières de travail qui constituent la contrepartie des habilitations découlant des articles 14 et 15.

Mise en œuvre de la protection des données (art. 17–22)

Art. 17

1. La responsabilité dont il est question à l'article 17 doit être comprise dans un sens large. Responsabilité avant tout administrative, elle constitue également le point de départ de la responsabilité civile réglée à l'article 28, ainsi que d'une éventuelle responsabilité disciplinaire.
2. De façon générale, la responsabilité de la protection des données est l'affaire de chaque organe qui traite des données, à quelque niveau que ce soit (al. 1). Elle consiste à respecter, lors de chaque traitement, l'ensemble des obligations découlant de la présente loi et, le cas échéant, d'autres dispositions relatives à la protection des données.
3. Cette règle générale relative à la responsabilité est complétée dans la loi par l'institution d'un responsable pour chaque fichier (notion définie à l'art. 3 let. g), qui devra déclarer celui-ci (art. 19 al. 1) et assurer notamment l'exercice par les personnes concernées de leur droit d'accès (art. 23 al. 1).
4. L'alinéa 2 traite du problème du partage des responsabilités en cas de traitement conjoint.
   On parle de traitement conjoint à partir du moment où, pour un fichier, il existe, en plus du responsable du fichier, au moins un participant (cf., sur la notion de participant, art. 3 let. h). Il existe toutefois diverses catégories de traitement conjoint. La plus simple est celle où il y a un responsable du fichier et un ou plusieurs participants. Mais il est également possible, par exemple, que plusieurs organes soient sur le même rang, chacun étant à la fois responsable pour une partie déterminée du fichier et participant pour d'autres parties.
   Devant la multiplicité des possibilités de traitement conjoint, il paraît difficile de poser des règles générales relatives au partage des obligations relevant de la protection des données. L'article 17 alinéa 2 se limite donc à exiger que la question soit résolue par les organes concernés dans chaque cas d'espèce, sur la

base d'une évaluation du système que ces organes désirent mettre en place. La déclaration (ou, éventuellement, les déclarations, s'il faut considérer qu'il s'agit de plusieurs fichiers) constitue l'instrument adéquat pour régler la répartition des fonctions et des responsabilités (art. 19 al. 2 let. e).
Cette répartition devra également porter sur l'organisation de l'exercice du droit d'accès par les personnes concernées (à toutes les parties du fichier) et des droits en cas d'atteinte.

Art. 18

1. Les services de l'administration font fréquemment appel à la collaboration d'autres organes ou de personnes privées pour traiter leurs données. Cette collaboration peut porter sur la partie technique du traitement, qui sera souvent assurée par un centre de calcul; elle peut aussi concerner tout ou partie du traitement matériel des données, notamment la collecte de celles-ci. Dans tous les cas, la protection et la sécurité des données qui se trouvent en mains du mandataire doivent être garanties. Sont engagées aussi bien la responsabilité du mandataire que celle du mandant.
2. Lorsque le mandataire est un organe public soumis à la loi, sa responsabilité est clairement établie en vertu de l'article 17 alinéa 1.
Lorsque tel n'est pas le cas, l'article 18 alinéa 2 exige que l'octroi du mandat fasse l'objet d'un contrat, dans lequel ces problèmes seront réglés.
Le contrat n'est cependant pas nécessaire lorsque le mandataire est soumis à une législation assurant une protection suffisante (al. 2 i.f.). A cet égard, une certaine équivalence doit être exigée; par exemple, les dispositions de la loi fédérale relatives au traitement de données par des personnes privées consacrent un régime plus souple que celui instauré par le projet, et l'octroi d'un mandat à une personne privée reste soumis à l'exigence d'un contrat.
3. L'organe public qui attribue le mandat n'est pas déchargé de la responsabilité en matière de protection des données (al. 1).
D'une part, c'est sur lui que repose la légitimité du traitement, c'est lui qui est responsable de la compatibilité fondamentale du traitement avec les principes généraux de la protection des données. Dans cette perspective, l'article 23 alinéa 3 précise en outre que c'est à l'organe qui fait traiter des données par un tiers d'assurer le respect du droit d'accès.
D'autre part, le mandant doit exercer une responsabilité que l'on pourrait comparer, dans une analogie avec la responsabilité civile, aux précautions que l'employeur doit prendre vis-à-vis de ses auxiliaires: il doit choisir avec soin le tiers auquel il entend confier ses données, il doit lui donner toutes les instructions adéquates pour l'accomplissement de son mandat, et il doit exercer, dans la mesure du possible, la surveillance nécessaire pour que les instructions données soient respectées.

Art. 19

1. Sur le rôle et l'importance de la déclaration des fichiers, cf. supra chapitre II.A, N° 1 et 6.
2. Le responsable du fichier, qui est soumis à l'obligation de déclarer, est défini à l'article 3 let. g.

3. La déclaration devant intervenir avant la mise en exploitation du fichier (art. 19 al. 1), une disposition transitoire est nécessaire pour les fichiers existant au moment de l'entrée en vigueur de la loi (art. 33).
4. Le projet fait coïncider, en ce qui concerne les indications à fournir au sujet des fichiers, ce qui est déclaré (art. 19 al. 2), ce qui est enregistré (art. 21 al. 1) et ce qui est rendu accessible au public (art. 21 al. 3). Le contenu de la déclaration correspond dès lors à un minimum.
Cette solution satisfait les divers intérêts en présence:
   a) La charge administrative imposée au responsable du fichier ne va pas au-delà de la formulation de renseignements qu'il doit de toute façon être en mesure de donner.
   b) Le public a à disposition les informations sur les fichiers susceptibles de l'intéresser.
   c) L'autorité de surveillance n'est pas d'emblée submergée sous une masse de renseignements difficile à gérer; pour le reste, elle dispose d'un pouvoir d'investigation qui lui permet d'obtenir tous les compléments d'informations qu'elle juge nécessaires (art. 31 al. 3).
5. Au sujet des informations mentionnées à l'alinéa 2, on peut encore faire les remarques suivantes:
   a) La base légale (let. b) est à comprendre dans le sens défini à l'article 4.
   b) En ce qui concerne la répartition des responsabilités (let. e), cf. supra commentaire de l'article 17, N° 4. La répartition des responsabilités n'a de sens qu'en présence de participants; cela étant, il faut préciser que les participants pourront également être, simultanément, des responsables partiels (d'une partie) du fichier.
   c) Les destinataires réguliers (let. f) sont aussi bien les bénéficiaires d'une procédure d'appel que les organes auxquels sont régulièrement transmises des informations.
6. L'article 19 alinéa 3 vise à une plus grande transparence. Il complète l'état d'information des collectivités participantes tout en donnant la possibilité aux membres de ces collectivités d'être renseignés sur place de façon exhaustive (cf. art. 21 al. 2 i.f.).

Art. 20

1. Cette disposition a pour but de limiter la charge administrative que comporte l'établissement des déclarations de fichiers, en supprimant l'exigence d'une telle déclaration pour certaines catégories de fichiers qui ne présentent manifestement pas de risques pour les droits des personnes concernées.
2. A l'exception des instruments de travail personnels (let. e), les fichiers exemptés de l'obligation de déclarer à l'alinéa 1 sont des fichiers qui n'ont pas besoin de la publicité du registre pour être connus par les personnes concernées.
3. Sont considérés comme instruments de travail personnels (let. e) les notes personnelles qu'un collaborateur utilise dans l'accomplissement de sa tâche, mais qui ont un caractère intransmissible et ne sont pas utilisables par un tiers.

4. Les copies du fichier qui visent uniquement un but de sauvegarde font partie du fichier, et n'ont pas à être déclarées, sans qu'il soit nécessaire de le mentionner dans la loi.
   Par ailleurs, lorsque des fichiers individuels constituent de simples applications d'un logiciel ou d'un fichier type et que les déclarations de ces fichiers seraient identiques, il est possible d'envisager une déclaration globale du logiciel ou du fichier type.

Art. 21

1. De même que sur le plan fédéral, le registre est conçu comme une compilation des déclarations de fichier, à laquelle est joint un répertoire. L'importance du registre à mettre en place dépend du nombre de déclarations.
2. L'alinéa 2 permet d'atteindre, avec un minimum de moyens, un double objectif.
   D'une part, le fait que les communes doivent tenir un registre de leurs déclarations leur permet de se rendre compte du nombre et de la nature des fichiers que leurs organes gèrent.
   D'autre part, pour leurs administrés, les communes sont dans tous les cas le lieu ordinaire de consultation du registre, même lorsque c'est l'autorité cantonale qui tient le registre original de leurs déclarations (cf. art. 29 al. 2).
3. La publicité du registre (al. 3) constituera, dans la majeure partie des cas, le point de départ du droit d'accès des personnes concernées. Toutefois, le droit d'accès peut également être exercé à l'égard des fichiers non déclarés.

Art. 22

1. Les mesures organisationnelles et techniques visent à assurer la sécurité des données sous l'angle de la protection des personnes. Il s'agit donc en soi de mesures de protection des informations elles-mêmes, mais dans un but de protection de la personnalité.
2. De façon générale, les données – qu'elles figurent dans des fichiers ou dossiers manuels ou dans un système informatisé – doivent être protégées contre les risques qui, mettant en cause leur confidentialité, leur disponibilité ou leur exactitude, peuvent aboutir à un traitement illicite.
   Les principaux risques sont la perte accidentelle, la destruction accidentelle ou non autorisée, des erreurs techniques, la falsification, le vol, l'utilisation ou l'accès illicites, la modification ou la copie non autorisées.
3. Les mesures techniques et d'organisation, entre lesquelles il est difficile d'établir une stricte distinction, recouvrent des mesures telles que l'aménagement des lieux, le choix du matériel, les procédures d'identification des usagers et de contrôle des transactions, les évaluations périodiques, la constitution de copies de sauvegarde, etc.
   En ce qui concerne plus particulièrement les traitements automatisés, il s'agira notamment des mesures qui sont prévues sur le plan fédéral à l'article 9 OLPD:
   - contrôle des installations à l'entrée, afin que seules les personnes autorisées aient accès aux locaux et aux installations concernés;

   - contrôle des supports de données, lesquels ne doivent pas pouvoir être lus, copiés ou modifiés par des personnes non autorisées;
   - contrôle du transport des données lors de leur communication;
   - contrôle de communication, qui permette l'identification du destinataire;
   - contrôle de mémoire, destiné à empêcher les accès non autorisés au contenu de la mémoire d'un système informatisé;
   - contrôles d'utilisation et d'accès, garantissant que seules les personnes autorisées ont accès aux seules données dont elles ont besoin;
   - contrôle d'introduction, tendant à assurer qu'un contrôle a posteriori des données introduites dans le fichier ou le système soit possible.
4. L'importance des moyens mis en œuvre doit être appréciée en fonction du principe de proportionnalité, sur la base de critères tels que le but, la nature et l'étendue du traitement, la nature des données traitées, ou encore le développement technique des installations utilisées.
5. Il revient en principe à chaque organe public d'évaluer les risques engendrés par les traitements de données qu'il effectue, et de prévoir des mesures techniques et organisationnelles appropriées. Toutefois, il paraît judicieux de poser des règles minimales en la matière. Il incombe au Conseil d'Etat de les édicter et de les adapter à l'évolution de la technique (al. 2).

Droits des personnes concernées (art. 23–28)

Art. 23

1. Le droit d'accès constitue en quelque sorte un «contre-droit» par rapport à l'habilitation de l'organe à traiter les données. Il est un droit subjectif strictement personnel. Ce qui signifie, d'une part, qu'un mineur ou un interdit capable de discernement peut l'exercer sans le consentement de son représentant légal, et, d'autre part, que nul ne peut y renoncer à l'avance.
   Pour les personnes morales, le droit d'accès sera exercé par les organes compétents selon les règles ordinaires du droit privé.
2. Le droit d'accès porte sur toutes les données qui figurent dans un fichier ou auxquelles un fichier permet d'accéder (cf. la notion large de fichier définie à l'art. 3 let. f). Il s'étend également aux fichiers qui, en vertu de l'article 20, n'ont pas à être déclarés.
   Son exercice n'est en principe soumis à aucune condition:
   a) Le requérant n'a pas à justifier sa demande (sauf s'il s'agit de consulter des données archivées: art. 25 al. 2 i.f.).
   b) Il n'est pas tenu de se référer, dans sa requête, à un fichier déterminé. Il peut demander à accéder à tous les fichiers dont l'organe public abordé est le responsable; il incombe alors à cet organe de guider le requérant vers les fichiers qui peuvent l'intéresser. En revanche, une demande ne peut pas être adressée à une administration dans son ensemble, ni à un organe supérieur pour tous les fichiers dont des organes subordonnés sont les responsables.

3. La personne concernée doit pouvoir accéder à toutes les données contenues dans un fichier ou dans les dossiers qui en dépendent. De ce point de vue, il appartient au responsable du fichier de prendre les mesures nécessaires pour assurer l'exercice effectif du droit d'accès. On peut faire à ce sujet les remarques suivantes:

   a) Selon la jurisprudence, «le droit de l'intéressé à être renseigné sur les données recueillies à son sujet par une autorité s'étend à la fois aux données de base, telles qu'elles sont enregistrées, et à celles qui résultent de leur traitement, en d'autres termes aux analyses et appréciations que les autorités ont faites en se fondant sur des données recueillies par elles, et qu'elles ont consignées dans leurs dossiers» (ATF 113 Ia 257ss, 265). En matière de personnel, par exemple, les résultats d'une analyse graphologique devront être communiqués.

   b) La personne concernée a le droit d'accéder à toutes les parties du fichier. En cas de pluralité de participants, on peut imaginer différents procédés: soit chaque participant octroiera le droit d'accès pour sa part, soit un organe sera désigné pour assurer le droit d'accès pour l'ensemble du fichier. L'important est que la question soit expressément réglée par les organes concernés dans la déclaration du fichier (art. 17 al. 2 et art. 19 al. 2 let. e).

   c) L'accès aux données traitées par un tiers doit également être garanti (al. 3). L'alinéa 3 rappelle en fait un principe déjà posé à l'article 18, à savoir que le responsable d'un fichier ne saurait échapper à ses obligations en confiant à un tiers le soin de traiter ses données.

Art. 24

1. La manière d'introduire une demande d'accès n'est pas réglée expressément dans le projet et dépendra des circonstances.
   En revanche, la loi exige la vérification de l'identité du requérant (al. 1): le droit d'accès pourrait, à défaut d'une telle vérification, jouer un rôle parfaitement opposé à celui pour lequel il est instauré.

2. La règle selon laquelle les renseignements sont fournis par écrit (al. 2), généralement sous forme de photocopie ou – s'agissant de données informatisées – d'une impression de celles-ci, n'est pas absolue. Si la personne concernée est d'accord, ils peuvent être communiqués oralement, notamment lorsque les données sont peu nombreuses. Quant à la consultation directe du fichier ou du dossier, qui suppose l'accord des deux parties, elle constitue dans certains cas la procédure la plus simple et la plus économique; elle devra être accompagnée des explications nécessaires.

3. Par rapport aux données enregistrées, les renseignements doivent être exacts et complets. Par exemple, le responsable du fichier ne peut pas se prévaloir du fait que les données sont périmées et auraient dû être détruites pour limiter la communication.
   La communication doit également être faite sous une forme compréhensible pour le destinataire. A cet égard, il faut rappeler que le responsable du fichier doit tenir compte, lors de l'organisation du fichier, des impératifs du droit d'accès.

4. L'accès indirect prévu pour les données sur la santé (al. 3) vise à empêcher ou à atténuer les effets néfastes que la communication de certains renseignements pourrait avoir sur les personnes concernées. Le choix entre l'accès direct et l'accès indirect appartient au responsable du fichier, alors que le choix du médecin appartient à la personne concernée.

5. L'exercice du droit d'accès ne peut en principe dépendre du prélèvement d'un émolument (al. 4). Si des exceptions sont nécessaires, notamment dans des cas d'abus (par exemple, répétition des demandes à intervalles rapprochés), il revient au Conseil d'Etat de les établir.

Art. 25

1. Les restrictions du droit d'accès doivent obéir au principe de proportionnalité. C'est ainsi qu'un refus de toute communication ne pourra être prononcé que si une mesure moins incisive, par exemple le caviardage de certains passages, n'est pas suffisante pour protéger les intérêts en jeu.

2. Les archives peuvent exiger que le requérant justifie sa demande d'accès à des documents qui ne sont pas encore accessibles au public en vertu de la législation y relative (al. 2). Avant d'octroyer le droit d'accès, elles consulteront au préalable le service qui a déposé les documents concernés, afin qu'il se prononce sur l'existence d'une restriction à la communication au sens de l'alinéa 1.

Art. 26

1. La réglementation prévue dans cette disposition, inspirée des actions de droit privé instituées par l'article 28a du code civil, donne à chaque personne concernée les moyens juridiques d'exiger que les traitements de données soient effectués conformément à la loi.

2. Les lettres a et b de l'alinéa 1 ont une fonction protectrice et correctrice, alors que la constatation du caractère illicite d'un traitement (let. c) sert aussi à des fins probatoires, notamment en vue d'assurer la réparation d'un éventuel préjudice.

3. En vertu de la maxime d'office (art. 45 CPJA), il incombe en principe à l'organe public d'établir la véracité des informations qu'il détient, la personne concernée étant toutefois tenue de collaborer à l'établissement des faits (art. 47 CPJA). Lorsque ni l'exactitude ni l'inexactitude des données ne peuvent être démontrées – notamment parce que ces dernières comportent une appréciation – et que l'organe public a néanmoins un intérêt légitime à les conserver, la lettre b de l'alinéa 2 offre une possibilité de résoudre le conflit.

4. La possibilité offerte par l'alinéa 2 let. c est également inspirée de l'article 28a du code civil, et permet notamment d'exiger qu'une rectification des données soit effectuée auprès des destinataires réguliers de celles-ci.

5. Lorsque les données sont archivées, leur rectification ou leur destruction s'opposent aux intérêts historiques qui justifient l'archivage. Comme, dans un tel cas, le principe de l'exactitude ne revêt plus la même importance que lors d'un traitement actif, l'alinéa 3 prévoit une exception aux droits découlant de l'alinéa 2 let. a.

Art. 27

Les voies de recours contre les décisions prises en matière de protection des données sont les voies ordinaires avec en principe, comme dernière instance cantonale, le Tribunal administratif. La commission de la protection des données n'est donc pas, contrairement à la Commission fédérale de la protection des données et à certaines commissions cantonales, une commission de recours.

Art. 28

1. L'alinéa 1 fait de la violation des dispositions de la loi sur la protection des données un acte illicite au sens de l'article 6 de la loi du 16 septembre 1986 sur la responsabilité civile des collectivités publiques et de leurs agents (RSF 16.1).
2. La possibilité offerte à l'alinéa 2, qui constitue le pendant de celle qui est prévue à l'article 26 alinéa 2 let. c, s'ajoute aux prestations financières que la personne concernée peut obtenir en vertu de l'alinéa 1.

Surveillance (art. 29–32)

Art. 29

1. Il existe divers modèles d'autorité de surveillance. Les cantons romands ont généralement opté pour une commission, alors que les cantons alémaniques ont pour la plupart institué un préposé. Le projet prévoit, quant à lui, une solution mixte, combinant l'indépendance et la légitimation, face à l'administration, d'une commission élue par le Grand Conseil, avec le professionnalisme et la disponibilité d'un préposé.
   Largement approuvée lors de la procédure de consultation, cette organisation mixte a néanmoins été sensiblement allégée par rapport à l'avant-projet: d'une part, l'on a renoncé à faire de la présidence de la commission une fonction semi-professionnelle, confiée à un juge qui aurait dû être libéré à cet effet d'une partie de sa charge; d'autre part, l'on a concentré sur le préposé des tâches que l'avant-projet confiait pour partie à des préposés internes, dont il prévoyait l'institution notamment dans chaque Direction de l'administration cantonale.
2. La solution retenue sur le plan cantonal (al. 1) est donc celle d'une autorité de surveillance à deux composantes (une commission et un préposé), qui exerce sa tâche auprès des organes et établissements de l'administration cantonale, ainsi que des communes qui n'ont pas leur propre autorité de surveillance (al. 2 i.f.).
3. Quant aux communes qui décident d'instituer leur propre autorité de surveillance, elles en déterminent librement l'organisation (al. 2). L'autorité communale de surveillance devra toutefois être indépendante du conseil communal et de son administration, et jouir de compétences comparables – toutes proportions gardées – à celles de l'autorité cantonale.

Art. 30

1. L'élection des membres de la commission par le Grand Conseil (al. 1) est souhaitable pour deux raisons. D'une part, elle garantit l'indépendance de l'autorité de surveillance vis-à-vis de l'Exécutif cantonal et de l'administration qui en dépend. D'autre part, elle assure à l'autorité de surveillance une plus grande légitimité par rapport aux communes.
   Le droit de proposition au Conseil d'Etat a pour but, quant à lui, d'associer cette autorité au choix des membres de la commission et d'assurer que ce choix se fasse d'abord en considération des compétences professionnelles requises, sans toutefois perdre de vue la pluralité politique. Il paraît souhaitable, à cet égard, que la commission soit présidée par un juriste et qu'elle comprenne en outre au moins une personne ayant une formation d'informaticien et une personne bénéficiant d'une expérience approfondie de l'administration.
   Dans les autres cantons romands qui ont institué une commission de surveillance, les membres de celle-ci sont désignés soit uniquement par le parlement (Valais), soit en partie par le parlement et en partie par l'exécutif (Genève, Jura), soit uniquement par l'exécutif (Neuchâtel).
2. La commission exerce les fonctions de l'autorité de surveillance qui exigent une légitimation accrue: avis au Grand Conseil ou au Conseil d'Etat (let. b); injonctions aux organes de l'administration (let. c); haute surveillance sur les communes qui ont institué leur propre autorité de surveillance (let. d).
   Elle fait rapport au Grand Conseil et peut, à l'instar du préposé fédéral (art. 30 al. 2 LPD), s'adresser, s'il en va de l'intérêt général, directement au public (al. 3).

Art. 31

1. Le préposé à la protection des données, nommé par le Conseil d'Etat (al. 1), devra être juriste de formation et posséder de bonnes connaissances en informatique. Il devra maîtriser les deux langues officielles.
2. C'est sur le préposé que se concentrera l'essentiel de l'activité courante de surveillance et de conseil en matière de protection des données, dans l'administration cantonale et auprès des communes.
   Outre les vérifications qu'il sera appelé à effectuer auprès des organes publics (al. 2 let. a), outre ses fonctions de conseil auprès de ces mêmes organes (al. 2 let. b) et des personnes concernées (al. 2 let. c), il devra également organiser la procédure de déclaration des fichiers (art. 20 al. 1) et établir le registre (art. 21 al. 1), tâches d'une ampleur certaine si l'on se réfère aux expériences faites en la matière par d'autres cantons.
   Placé sous l'autorité de la commission, qui dirigera son activité et pourra lui confier certains travaux spécifiques (art. 30 al. 2 let. a et art. 31 al. 2 let. d), le préposé lui fera régulièrement rapport (art. 31 al. 2 let. e), tout en assurant son secrétariat (art. 30 al. 1 i.f.).
3. L'alinéa 3 attribue au préposé les pouvoirs nécessaires à l'accomplissement de ses tâches.

Droit transitoire (art. 33 et 34)

Art. 34

Cette disposition tient compte de la situation des petites communes qui ne disposent pas d'un secrétariat permanent, et des risques atténués que présentent les fichiers manuels par rapport aux fichiers automatisés.

Elle signifie, a contrario, que les déclarations de fichiers et la tenue d'un registre sont exigées des communes à partir du moment où celles-ci commencent à s'informatiser.

Modification de la loi sur le controle des habitants (art. 35)

Une modification des dispositions de la loi sur le contrôle des habitants relatives à la protection des données est nécessaire pour deux raisons. D'une part, il s'agit d'adapter ces dispositions à l'existence d'une loi générale sur la protection des données en établissant un renvoi général à cette loi (art. 18a nouveau LCH), tout en maintenant un régime spécifique pour les communications. D'autre part, une enquête effectuée auprès de l'association cantonale des secrétaires et caissiers communaux a démontré que les dispositions existantes étaient souvent mal comprises.

Art. 16 al. 2 LCH

L'habilitation générale de communiquer des données à des organes publics est limitée aux cas d'espèce, en harmonie avec l'article 10 alinéa 1 LPrD. Il s'ensuit qu'une communication régulière à de tels organes n'est autorisée que si une disposition légale le prévoit.

Art. 17 LCH

1. L'essentiel des communications de données à des particuliers ou à des organisations privées se fait par l'intermédiaire du contrôle des habitants.
2. L'alinéa 1 constitue une disposition légale au sens de l'article 10 alinéa 1 LPrD. Il dispense le préposé au contrôle des habitants de s'interroger lors de chaque communication sur l'application du principe de finalité.
3. Les alinéas 2 et 3 visent la communication de données concernant une pluralité de personnes définie par un critère général (par exemple, la communication des noms de toutes les personnes habitant la commune *qui sont nées durant l'année 1950).*
   Cette communication est doublement limitée. D'une part, seules certaines des données mentionnées à l'alinéa 1 peuvent être transmises. D'autre part, cette transmission est soumise à la condition que les données soient utilisées à des fins idéales dignes d'être soutenues.
   La décision y relative est placée dans la compétence du conseil communal, lequel aura donc à apprécier de cas en cas si les fins invoquées répondent à cette condition.
   Les réglementations communales édictées en la matière sur la base de l'actuel article 17 LCH deviendront caduques dès l'entrée en vigueur de la loi.
4. L'alinéa 4 dispense le préposé au contrôle des habitants de vérifier lors de chaque communication l'exactitude des données.

Art. 18 LCH

1. Le droit de blocage que chaque habitant peut faire valoir constitue la contrepartie des assouplissements prévus à l'article précédent.
2. La lettre b de l'alinéa 2 est inspirée de la règle prévue à l'article 19 alinéa 1 let. d LPD.

Modifications de la loi sur le statut du personnel de l'Etat et de la loi sur les communes (art. 36 et 37)

Art. 13 al. 3 LStP

Il n'appartient pas au législateur de la protection des données de revoir le problème posé par l'article 13 LStP, disposition qui traite, dans un cadre peu approprié, de la communication de renseignements par les collaborateurs de l'Etat. Toutefois, il paraît important d'établir un lien entre l'habilitation générale prévue à l'article 13 et la loi sur la protection des données.

Ainsi, lorsque les renseignements portent sur des données personnelles, la communication de celles-ci est subordonnée non seulement aux conditions posées aux alinéas 1 et 2, mais encore à celles prévues par la loi sur la protection des données.

Art. 49a LStP et 75bis LCo

1. Aussi bien l'Etat que les communes sont soumis à la loi sur la protection des données lorsqu'ils traitent des informations au sujet de leurs collaborateurs:
   - pour ce qui concerne les collaborateurs engagés par contrat de droit public, en raison du renvoi figurant aux articles 49a alinéa 2 nouveau de la loi du 22 mai 1975 sur le statut du personnel de l'Etat (RSF 122.70.1, ci-après LStP) et 75bis alinéa 2 nouveau LCo;
   - pour ce qui concerne les collaborateurs engagés par contrat de droit privé, par application directe de la loi sur la protection des données.
2. L'administration des rapports de service (art. 49a al. 1 LStP et art. 75bis al. 1 LCo) comprend notamment les qualifications périodiques dont doivent faire l'objet les collaborateurs.
3. La nécessité d'établir un règlement relatif au traitement des données concernant le personnel de l'Etat tient au fait que de nombreuses questions spécifiques doivent être réglées, notamment:
   - la répartition des responsabilités entre l'Office du personnel, les autorités d'engagement et les autres organes chargés de tâches de gestion du personnel;
   - les caractéristiques des différentes banques de données relatives au personnel, ainsi que les relations établies, d'une part, entre ces différentes banques de données et les dossiers personnels de chaque collaborateur, et, d'autre part, entre les banques de données elles-mêmes;
   - les questions liées aux dossiers de candidature;
   - le traitement des données médicales;
   - la communication de données à des tiers;
   - les contrôles préalables de sécurité pour certaines fonctions;
   - l'information du personnel et de ses représentants sur les traitements de données concernant les collaborateurs de l'Etat.

Art. 168 I ch. 21 LCo

La modification de l'article 168 LCo intervient dans le cadre de l'adaptation de la législation concernant les rapports Eglises-Etat aux exigences de la protection des données (voir ci-dessous).

Modification de la législation concernant les relations Eglises-Etat (art. 37, 38 et 40)

1. La loi sur la protection des données ne doit pas remettre en question la collaboration administrative de l'Etat et des communes avec les Eglises reconnues: cette collaboration constitue un élément du statut de droit public des Eglises reconnues.
   Or cette collaboration joue un rôle essentiel aussi bien lors de l'établissement du registre des corporations ecclésiastiques que pour le calcul et la perception des impôts ecclésiastiques. Elle comporte, dans ces deux cas, la communication aux corporations ecclésiastiques de données relatives à l'appartenance confessionnelle des personnes concernées. Comme ces données sont des données sensibles au sens de l'article 3 let. c LPrD, il convient de régler explicitement leur communication dans la loi. Bien que la loi cantonale sur la protection des données ne prévoie pas, contrairement à la loi fédérale (cf. art. 17 al. 2 LPD), l'exigence d'une base légale formelle pour le traitement de données sensibles, l'opportunité d'édicter une telle base légale dans le cas d'espèce découle d'un impératif de clarté et de transparence.
2. Dans l'état actuel de la législation, la seule disposition légale autorisant la communication, à des corporations ecclésiastiques, de données relatives à l'appartenance confessionnelle des personnes est l'article 13 de la loi du 13 mai 1966 concernant l'organisation de l'Eglise évangélique réformée du canton de Fribourg (RSF 192.1).
   Il convient donc, notamment pour ce qui concerne les paroisses catholique, de compléter le régime transitoire applicable jusqu'à l'entrée en vigueur, dans son régime ordinaire, de la loi sur les rapports Eglises-Etat. Tel est l'objet de la modification de l'article 168 LCo par l'article 37 LPrD, ainsi que de l'introduction, par l'article 40 LPrD, d'un article 33a dans la loi du 10 mai 1963 sur les impôts communaux et paroissiaux (RSF 632.1).
3. Quant à la loi sur les rapports Eglises-Etat, elle contient déjà une base légale suffisante pour la communication des informations nécessaires au calcul et à la perception des impôts ecclésiastiques (art. 17 al. 1 LEE). L'article 38 se limite donc à préciser le contenu de l'article 24 alinéa 1 LEE pour ce qui concerne l'établissement du registre des membres des corporations ecclésiastiques.

Modification de la loi sur la police cantonale (art. 39)

1. Le Conseil d'Etat s'est engagé, lors de l'adoption de la loi sur la police cantonale, à régler en relation avec la loi sur la protection des données les questions spécifiques qui se posent à ce sujet dans le cadre du travail de la police. L'article 39 répond à cet engagement, tout en clarifiant les relations entre la loi sur la police cantonale, le code de procédure pénale et la loi sur la protection des données.

2. La nature particulière des tâches de la police exige, d'une part, certaines dérogations aux règles générales de la protection des données, et, d'autre part, des concrétisations de ces règles ainsi que des prescriptions spécifiques d'ordre matériel et procédural, ayant pour but de contrebalancer les dérogations susmentionnées.
3. Des dérogations sont nécessaires en particulier sur les points suivants:
   a) Les règles sur la collecte de données doivent être assouplies: si, en raison de la précision figurant à l'article 9 alinéa 1 deuxième phrase LPrD, il n'est pas nécessaire de dire expressément que la nature des tâches de la police exigera régulièrement une collecte auprès de tiers, en revanche une dispense du principe de la collecte reconnaissable s'impose (art. 38b al. 1 LPol).
   b) La conservation des données dans des fichiers organisés en vue de la réutilisation de celles-ci constitue une spécificité du travail de la police, pour laquelle il convient de créer une base légale (art. 38d al. 1 LPol).
   c) Dans certains cas, une motivation détaillée de la décision refusant le droit d'accès (art. 25 al. 3 LPrD) peut révéler indirectement ce qui doit être tenu secret; la plupart des situations concernées relèvent des compétences de la police fédérale (sécurité intérieure) ou devraient prochainement être réglées par la législation fédérale (réglementation relative à la lutte contre le crime organisé). Dans les rares cas où la question pourrait dès lors encore se poser sur le plan cantonal, la motivation pourra être réduite à la simple invocation de l'article 25 alinéa 1 let. a LPrD, étant entendu que la personne concernée aura la possibilité, dans le cadre d'un recours contre le refus du droit d'accès, de faire examiner également le bien-fondé de ce procédé.
4. En contrepartie, les dispositions de la loi sur la protection des données sont précisées et complétées en matière de collecte et de communication de données (art. 38c et 38g LPol), ainsi que sur les points suivants:
   - attribution au directeur de la police de la compétence de fixer la durée de conservation des données de police (art. 38d al. 2 LPol);
   - obligation d'organiser les fichiers de police selon certaines règles, et de prévoir un règlement de traitement pour les fichiers de recherche criminelle (art. 38e et 38f LPol).

Art. 38a LPol

1. L'alinéa 1 constitue une base légale au sens de l'article 4 LPrD. Il renvoie, pour la définition des tâches de la police, à l'article 2 LPol, et établit une distinction entre les données de police (données nécessaires à l'accomplissement des tâches propres de la police) et les autres données traitées par la police (données concernant le personnel, les fournisseurs, etc.), qui ne posent pas de problèmes particuliers.
2. Sous l'angle de la législation applicable, les tâches de police judiciaire sont régies par le code de procédure pénale. Il s'ensuit qu'en vertu de son article 2 alinéa 2 let. b, la loi sur la protection des données ne devrait pas s'appliquer à ces tâches.
   Toutefois, dans le travail concret de la police, l'activité préventive ne peut pas toujours être clairement distinguée de l'activité de police judiciaire; en outre, la

police conserve, dans certaines limites, les données qu'elle a recueillies dans le cadre d'enquêtes judiciaires en vue de les réutiliser lors de nouvelles enquêtes; enfin, ni le code de procédure pénale en vigueur, ni le projet actuellement en préparation ne règlent de façon exhaustive la protection des données.
Il paraît dès lors indiqué d'inclure les tâches de police judiciaire dans le champ d'application de la loi sur la protection des données, étant entendu que les dispositions du code de procédure pénale primeront celles de la loi sur la protection des données lorsqu'elles porteront sur le même objet, notamment en ce qui concerne l'accès au dossier et le devoir de discrétion (al. 3).

Art. 38b LPol

1. L'alinéa 1 déroge à l'article 9 alinéa 2 LPrD. Cette dérogation, justifiée par la nature des tâches de la police, ne vise que l'observation ordinaire, sans engagement de moyens particuliers, portant, pour reprendre la formulation de l'art. 179 quater du code pénal, sur des faits pouvant être perçus sans autre par chacun.
2. Par contre, le recours à des moyens comportant une atteinte grave aux droits des personnes, et nécessitant de ce fait une base légale spécifique (engagement d'agents infiltrés ou utilisation de moyens techniques de surveillance, observation prolongée, etc.) n'est pas visé par cette disposition (al. 2). D'une part, cette question ne relève pas uniquement de la protection des données. Et, d'autre part, la Confédération est en train de préparer, dans le cadre des mesures de lutte contre le crime organisé, des dispositions légales concernant notamment les missions d'agents infiltrés et les formes particulières d'observation.

Art. 38c LPol

1. Cette disposition vise à empêcher la collecte de données sensibles en dehors d'une enquête (de police ou de police judiciaire) déterminée, pour des besoins futurs. Il s'agit à la fois d'une qualification de la nécessité de recueillir ces données et d'une précision relative à l'immédiateté des besoins pour lesquels ces données sont recueillies.
2. Par le biais de cette disposition est interdite la constitution de bases de données telles que des fichiers d'homosexuels, de prostituées, de clochards, etc.

Art. 38d LPol

1. La police doit, dans certaines limites, pouvoir réutiliser pour d'autres enquêtes les données recueillies lors d'une enquête déterminée. Il faut donc que ces données puissent être conservées de façon à pouvoir être réactivées. L'alinéa 1 fournit une base légale pour cette conservation, qui reste soumise aux règles de la protection des données (en particulier aux principes de proportionnalité et d'exactitude).
Quant à la réutilisation proprement dite, elle est soumise aux conditions générales prévues par la loi sur la protection des données – et notamment au principe de finalité (art. 5 LPrD) –, en raison du renvoi de l'article 38a alinéa 2 LPol.
2. En relation avec les données de police, le Tribunal fédéral a admis que le droit à l'oubli constitue un élément de la liberté personnelle (arrêt du 12 janvier 1990, in Semaine judiciaire 1990, p. 561ss, 565). La durée de conservation de ces données doit donc être limitée, le principe de proportionnalité exigeant qu'elles soient éliminées des fichiers et dossiers de police dès qu'elles ne sont plus nécessaires.
Il appartiendra au Directeur de la police de fixer des délais de conservation pour les différentes catégories de données de police (al. 2), en distinguant entre des délais généraux – au terme desquels les données devront faire l'objet d'un réexamen et ne pourront être conservées que si, dans le cas d'espèce, des motifs particuliers le justifient –, et des délais absolus de radiation.
3. La décision relative au mode d'élimination des données (archivage ou destruction) relève des Archives (cf. art. 13 du règlement concernant les Archives de l'Etat), étant rappelé que les dossiers de police archivés sont soumis à des délais de consultation spéciaux (art. 6 al. 1 let. b de ce règlement).

Art. 38e et 38f LPol

1. Ces dispositions, qui imposent à la police des obligations particulières dans l'organisation de la conservation des données, constituent une contrepartie de l'habilitation prévue à l'article 38d.
2. La distinction établie à l'article 38e al. 2 entre fichiers de police «ordinaires» (amendes d'ordre, accidents de la circulation, etc.) et fichiers de recherche criminelle s'impose du fait que ces derniers contiennent régulièrement des données qui sont à la fois très sensibles (poursuite pénale pour un crime ou un délit d'une certaine gravité) et inégalement vérifiées (la vérification progresse en cours d'enquête).
L'obligation de procéder à cette distinction a une double portée:
   a) Il doit exister une séparation logique entre les fichiers de recherche criminelle et les autres fichiers de police. Cela signifie que la police ne peut relier entre eux des fichiers appartenant à ces deux catégories. Demeure cependant ouverte la faculté de consulter de cas en cas, à des fins de recherche criminelle, des fichiers qui ne sont pas en soi tenus à de telles fins; l'accès direct à de tels fichiers devra être défini dans le règlement de traitement mentionné à l'article 38f (cf. art. 38f al. 2 let. d).
   b) Les fichiers de recherche criminelle doivent faire l'objet d'un règlement de traitement (art. 38f al. 1).
3. La police distingue, parmi le personnes enregistrées dans les fichiers de police criminelle, les «personnes avec antécédents» des autres personnes (plaignants, témoins, etc.). Sont considérés comme personnes avec antécédents les individus ayant commis ou étant soupçonnés d'avoir commis un crime ou un délit, pour autant que la nature de l'infraction ou les circonstances du cas d'espèce justifient leur enregistrement en tant que tels dans un fichier de recherche criminelle.
Cette distinction ne répond pas seulement à des besoins de recherche criminelle, mais aussi à des exigences de protection des données (principes de proportionnalité, d'exactitude, etc.). En particulier, chacun a un intérêt évident à ne pas être enregistré sans raison comme «personne avec antécédent».
C'est pourquoi la loi attribue un caractère normatif à la distinction susmentionnée. De ce fait, le règlement de traitement prévu à l'article 38f devra tenir

compte des particularités propres aux différentes catégories de personnes enregistrées, notamment en ce qui concerne les données qui peuvent être enregistrées et les autorisations d'accès.

4. Le règlement dont il est question à l'article 38f est un règlement de traitement de même nature que celui prévu à l'article 36 alinéa 4 let. a LPD. Il s'agit donc d'un acte interne, qui fixera de façon détaillée la structure du système et ses diverses composantes.
L'approbation par le directeur de la police permet à ce dernier de s'assurer que le règlement répond en tous points aux exigences de la protection des données, et d'exercer ainsi son pouvoir de contrôle.

Art. 38g LPol

1. L'alinéa 1 de cette disposition constitue un rappel qui recouvre différentes situations, notamment la communication de données aux autorités judiciaires, la communication de données dans le cadre de l'entraide judiciaire et la communication au préfet de données intéressant l'ordre public.
2. Les règles concernant la communication de données sur demande (al. 2) sont plus restrictives, dans le domaine de la police, que les dispositions générales de l'article 10 alinéa 1 LPrD. En effet, les dossiers de police sont en principe secrets (cf. art. 24 LPol, qui soumet de façon générale les affaires de police au secret de fonction), sous réserve des échanges d'informations que nécessite la collaboration de la police cantonale avec les organes de police de la Confédération et des autres cantons (cf., sur ce point, l'actuel art. 40 al. 2 LPol, remplacé par la disposition de la let. a de l'art. 38g al. 2).
3. La présomption de consentement mentionnée à la lettre d de l'alinéa 2 pourra notamment être admise dans le cadre de la recherche de personnes disparues.

Disposition finale (art. 41)

L'entrée en vigueur de la loi mettra fin au système de surveillance imposé par l'article 37 de la loi fédérale et mis en place par le décret du 7 mai 1993 instituant un délégué à la protection des données traitées en vertu du droit fédéral (RSF 17.2).

IV. CONSÉQUENCES FINANCIÈRES

1. Besoins en personnel

En raison de la situation financière de l'Etat, les moyens initialement prévus pour la mise en œuvre de la protection des données dans notre canton ont été réduits. C'est ainsi que le projet renonce, notamment, aux préposés internes dont l'avant-projet prévoyait l'institution, à temps partiel, dans les principaux secteurs de l'administration cantonale. Il n'en demeure pas moins que l'autorité de surveillance devra pouvoir compter sur la collaboration, dans les établissements et services, de répondants plus particulièrement chargés de pourvoir à l'application de la législation sur la protection des données.

La mise en place de l'autorité de surveillance exigera la création de deux postes de travail: celui du (ou de la) préposé(e) et celui d'un(e) secrétaire. Les tâches du préposé seront celles énumérées à l'article 31 du projet; le préposé aura à remplir ces tâches non seulement pour l'administration cantonale et les institutions qui en dépendent, mais sans doute aussi pour la plupart des communes. Quant au secrétaire, il aura, outre la charge d'assurer le secrétariat et la réception du bureau du préposé, à gérer le registre des fichiers et à tenir le procès-verbal de la commission. A noter que le nombre des fichiers à enregistrer devrait être de l'ordre de 600 pour l'administration cantonale et de plus de 1000 pour les communes.

2. Coûts

a) Dépenses répétitives (par année)

L'entrée en vigueur de la loi sur la protection des données entraînera la suppression de la fonction de délégué à la protection des données personnelles traitées en vertu du droit fédéral. Il s'ensuit qu'une partie seulement des dépenses de fonctionnement résultant de la mise en œuvre de la future loi seront des dépenses nouvelles.

Objet	Dépenses totales Fr.	Dont dépenses nouvelles Fr.
Rémunération du (de la) préposé(e) et du (de la) secrétaire, avec charges	182 000	122 000
Frais de bureau, documentation, déplacements, frais administratifs divers	10 000	2 000
Locaux (loyers et charges)	13 000	–
Mandats informatiques	10 000	
Total	215 000	124 000

b) Dépenses uniques

	Fr.
Machines et matériel de bureau, mobilier*, informatique*, imprimés, frais divers	28 000

* Une partie du mobilier, un ordinateur personnel ainsi que la bibliothèque pourront être repris de la déléguée à la protection des données personnelles traitées en vertu du droit fédéral.

c) Le Conseil d'Etat s'est demandé si le coût afférent à la surveillance, par l'autorité cantonale, des communes qui renoncent à instituer leur propre autorité de surveillance pourrait être facturé à celles-ci. Il y a renoncé, au vu du montant relativement faible que cela devrait représenter pour chaque commune. En revanche, il a décidé de prendre en compte ce coût dans la balance des charges qui sera établie dans le cadre du réexamen de la répartition des tâches entre l'Etat et les communes.