Rapport
présenté par la Direction de la justice au Conseil-exécutif, à l'intention du Grand Conseil, concernant la loi sur la protection des données

Introduction

L'utilisation toujours plus fréquente de techniques d'information modernes ainsi que la multiplication rapide et générale des tâches de l'Etat exigent l'élaboration de dispositions qui protègent l'individu contre l'usage abusif d'informations le concernant. La réglementation du traitement de données personnelles permettra en outre de rendre l'administration et les particuliers plus conscients de la protection des données et de pallier le malaise qu'éprouve le citoyen face aux possibilités techniques ouvertes par le traitement électronique des données. Il est donc important d'organiser l'activité des autorités de sorte que soit évité tout abus pouvant résulter du traitement de données personnelles. Cela signifie que l'activité d'information doit être limitée au nécessaire et que les personnes intéressées doivent avoir la possibilité de contrôler et de se défendre. Ces mesures servent aussi les intérêts bien compris de l'administration elle-même, qui par la présente loi se voit garantir l'obtention des données dont elle a besoin.
Le canton de Berne s'est bien vite rendu compte des dangers que pouvait présenter le traitement abusif de données et a le 13 septembre 1977 déjà édicté une ordonnance sur la protection des données. En juillet 1982, la Direction des communes a en outre arrêté un modèle de règlement sur la protection des données destiné aux communes. Au fil des années, les dispositions de protection cantonales se sont toutefois révélées insuffisantes. Le champ d'application de ces dernières, en particulier, se limite au traitement électronique des données et ne restreint donc en rien le traitement de données délicates au moyen de fichiers traditionnels. Les droits des personnes intéressées, tels que les prévoit l'ordonnance, sont en outre trop restreints et la surveillance exercée sur la protection des données insuffisante.
Le canton de Berne n'est pas le seul à avoir saisi l'importance de la protection des données. C'est ainsi que le 1er février 1983, sur mandat de la Conférence des directions cantonales de la justice et de la police, un groupe de travail a élaboré une loi-modèle cantonale sur la protection des données. Au niveau de la Confédération, le projet de loi fédérale sur la protection des données personnelles de décembre 1983, qui régit le traitement de données par les personnes de droit privé et par les organes de la Confédération, est parti en consultation. Nombreux sont les cantons qui se sont déjà donné leur loi sur la protection des données ou qui sont en train de l'élaborer.
Le 6 novembre 1980, le Grand Conseil a accepté une motion Cahenzli du 20 août 1980, qui demandait la création d'une loi sur la protection des données. Le 18 avril 1984, le Conseil-exécutif du Canton de Berne a désigné un groupe de travail, qui, sous la responsabilité de la Direction de la justice, était chargé d'élaborer un projet de loi bernoise sur la protection des données. Conformément au mandat donné au groupe de travail, le projet devait avoir pour base la loi-modèle précitée ainsi que l'ordonnance sur la protection des données aujourd'hui en vigueur. Parallèlement, il devait, dans la mesure du possible, être accordé avec le projet de loi fédérale sur la protection des données. Le groupe de travail se compose de représentants non seulement des différentes directions, mais aussi des milieux intéressés (Union syndicale, Union du commerce et de l'industrie).
Le 15 juin 1983, M. le député au Grand Conseil Haudenschild a déposé un postulat demandant la création d'une autorité de surveillance indépendante en matière de protection des données avant la promulgation de la loi. Suivant la proposition du Conseil-exécutif, le Grand Conseil a accepté l'intervention et a chargé le groupe de travail d'étudier la réalisation du postulat Haudenschild. Etant donné la relative rapidité avec laquelle le projet de loi prenait forme et les rapports étroits existant entre la conception d'une autorité de surveillance et les dispositions sur la protection des données, le Conseil-exécutif, sur proposition du groupe de travail, a décidé d'inclure les dispositions régissant l'autorité de surveillance dans la loi sur la protection des données.

Protection des données dans les administrations communales

La question est de savoir si l'application de la loi sur la protection des données doit s'étendre aux administrations communales. Désireux de préserver dans toute la mesure du possible l'autonomie des communes, le Conseil-exécutif a d'abord beaucoup hésité à soumettre ces dernières aux dispositions protectrices de la nouvelle loi. Cette hésitation était en particulier due au fait que certaines communes, Bienne en particulier, avaient fourni un remarquable travail de pionnier en légiférant sur la protection des données et qu'ainsi ces communes disposaient déjà d'une protection efficace des données. Ce point de vue n'a cependant pas résisté aux considérations suivantes. Tout d'abord, le canton doit édicter des dispositions unitaires pour protéger l'échange de données entre les communes d'une part et entre les communes et les autorités cantonales de l'autre, ce qui représente une première restriction de l'autonomie des communes. C'est par ailleurs le canton qui oblige les communes à recueillir des données, en particulier dans le domaine du contrôle des habitants. Il ne peut donc pas dénier toute responsabilité lorsqu'il s'agit de protéger ces données. Finalement, il convient de tenir compte des besoins du citoyen, qui ne comprend guère que les mêmes données traitées au niveau fédéral, cantonal ou communal jouissent à chaque échelon d'une protection différente, sans compter les inégalités existant entre les communes elles-mêmes. Si l'on songe que les mêmes données d'un citoyen sont en règle générale traitées par différentes autorités (p. e. commune d'origine, commune de domicile, domicile fiscal, canton, Confédération), il paraît évident qu'une certaine harmonisation des dispositions de protection s'impose. C'est pourquoi le champ d'application de la loi-modèle élaborée par les directeurs cantonaux de la justice et de la police s'étend aux communes. Les auteurs du présent projet ont respecté le principe de la loi-modèle tout en réservant aux communes des libertés considérables lorsque cela paraissait raisonnable. C'est ainsi que dans le domaine de la protection des données traitées par le contrôle des habitants, qui de toute la commune est l'organe qui

détient le plus de données, les communes se voient attribuer de larges compétences (art. 12). Elles désignent par ailleurs leur propre autorité de surveillance (art. 33), et donc gèrent leur propre registre (art. 18), ainsi qu'exercent de manière autonome d'importantes fonctions de surveillance dans la commune (art. 34). L'autorité de surveillance communale détient également les compétences définies à l'article 35 (cf. art. 37, 3e al.).

Résultats de la procédure de consultation

Une vaste procédure de consultation a été organisée au printemps 1985. La grande majorité des 54 organes et organisations qui y ont répondu se réjouissent de l'élaboration d'une loi sur la protection des données et se déclarent d'accord avec les grandes lignes du projet proposé. Rares sont les prises de position qui nient la nécessité d'une loi sur la protection des données ou qui prônent une réglementation nettement plus rudimentaire. Les échos positifs étaient par ailleurs très souvent accompagnés de propositions constructives d'amélioration du projet dont il a, dans toute la mesure du possible, été tenu compte lors du remaniement du premier jet.
La volonté d'inclure les communes dans le domaine d'application de la loi tout en leur réservant autant de marge de manœuvre que possible, a, en particulier, été très largement approuvée. Il est tout de même certaines voix isolées qui rejettent cette marge d'autonomie communale et d'autres qui désireraient faire entrer la protection des données dans la compétence quasi exclusive des communes. Le Conseil-exécutif, quant à lui, s'est prononcé pour le maintien de la solution prévue dans le projet initial. Pour ce qui était finalement du choix entre commission pour la protection des données et délégué à la protection des données, les milieux consultés ont présenté des avis divergents. Si la solution instituant une commission rallie la majorité des voix, certains auraient préféré renoncer à la création d'une nouvelle autorité de surveillance pour confier la surveillance de la protection des données à la Direction de la justice.

Commentaire article par article

Article premier

La présente loi a pour but de protéger le citoyen contre les abus dans le traitement de données par les autorités de l'Etat et des communes et par des organisations jouissant du même statut (art. 2, 5e al.). Ce n'est pas là un rempart qui protège contre tous les traitements de données personnelles, mais uniquement un bouclier destiné à éviter les traitements abusifs. Un traitement peut en particulier être qualifié d'abusif lorsqu'il enfreint la présente loi.

Article 2

L'introduction d'une nouvelle matière exige impérativement que certaines notions soient définies. Cette opération permet également de délimiter le champ d'application matériel d'un texte législatif. Les auteurs de la présente loi se sont appliqués, dans la mesure du possible, à reprendre les termes utilisés dans la loi-modèle, qui à son tour, correspond du point de vue terminologique au projet de loi fédérale.

1er alinéa

Il ressort du 1er alinéa que seules les données personnelles jouissent de la protection de la présente loi et que toutes les autres données (informations) sont exclues. La protection s'étend à toutes les personnes, qu'elles soient physiques ou morales. Sont également considérées comme données personnelles les indications relatives aux conditions matérielles d'une personne.

2e alinéa

La notion de «fichier» étant utilisée dans plusieurs dispositions de la présente loi, il convient de la définir. Ce terme recouvre à la fois les fichiers traditionnels et les fichiers électroniques.
S'il est vrai que ce sont les systèmes de traitement automatisés qui ont fait prendre conscience des problèmes juridiques que pose la protection des données, les principes élaborés n'en sont pas moins applicables aux méthodes de traitement manuel traditionnelles. Si ces dernières n'étaient pas soumises à la loi, les données sensibles pourraient être conservées dans des fichiers traditionnels et échapper ainsi à la protection générale de la loi. Le grand avantage du traitement automatisé des données, qui représente à la fois son grand danger dans l'optique de la protection des données, c'est sa rapidité, la multiplicité des possibilités qu'offre l'exploitation d'un fichier ainsi que la facilité avec laquelle différents recueils de données peuvent être connectisés. Par contre, si des mesures de sécurité techniques perfectionnées ont été développés à l'intention du traitement électronique des données, rien de tel ne protège le domaine des fichiers traditionnels. Il sera par ailleurs toujours plus difficile, vu l'évolution technique, de délimiter clairement le traitement manuel et le traitement automatique des données. Différents systèmes hybrides sont aujourd'hui déjà utilisés dans l'administration.

3e alinéa

En disant qu'«Est considérée comme traitement de données personnelles toute activité...» les auteurs ont tenté de souligner le fait que la loi protège les données à chaque étape de leur traitement, depuis l'acquisition jusqu'à l'archivage ou à la destruction (cf. art. 19).

5e alinéa

Sont par conséquent soumis à la présente loi tous les collaborateurs de l'Etat et des communes y compris les corporations de droit communal au sens de l'article premier de la loi sur les communes. Les présentes dispositions s'étendent également aux organisations et personnes de droit privé, dans la mesure où une tâche publique leur a été confiée.

Article 3

Les données personnelles se composent de données assez anodines, telles que nom et adresse, et de données particulièrement dignes de protection, dont l'utilisation peut facilement porter atteinte à la personnalité de leur propriétaire et qui donc paraissent nécessiter une protection particulière. En vertu de l'article 6, cette catégorie de données bénéficie d'une protection plus complète que les autres données personnelles. Les données personnelles bénéficiant toutes d'une protection efficace en vertu de la présente loi, il convient de rester très restrictif dans la définition des données particulièrement dignes de protection. Les auteurs de la présente loi ont renoncé à mentionner expressément les opinions et activités syndicales, car celles-ci sont de nature soit politique, soit philosophique.

Article 4

1er alinéa

La loi s'applique à tout traitement de données personnelles, quels que soient les moyens et méthodes utilisés.

2e alinéa

lettre *a*

Concerne avant tout la Banque cantonale et la Caisse hypothécaire. Ces deux instituts seront soumis à la future loi fédérale sur la protection des données dans le domaine privé; jusqu'à l'entrée en vigueur de cette loi fédérale, ils devront respecter les dispositions du Code civil garantissant la protection de la personnalité et jouissent ainsi du même traitement que les autres banques. La Banque cantonale et la Caisse hypothécaire sont toutefois aujourd'hui déjà soumises à l'autorité de surveillance en vertu des articles 32 ss. Cela signifie principalement que, jusqu'à l'entrée en vigueur des dispositions fédérales, l'autorité de surveillance exercera ses fonctions d'ombudsman également vis-à-vis des deux banques (cf. art. 34).

lettre *b*

Les calepins et agendas que certains fonctionnaires ou employés utilisent pour leur usage personnel exclusivement n'ont, pour des raisons qui touchent à la protection de la personnalité, pas été soumis aux dispositions de la présente loi.

lettre *c*

Les procédures civiles, administratives ou pénales pendantes ainsi que les procédures d'enquête des autorités de police sont régies par les lois spécifiques traitant des procédures respectives. Ce sont ces lois qui règlent le droit d'être entendu, le droit de consulter les dossiers ainsi que l'obligation de motiver. Elles prévoient le degré de publicité des procédures et décrivent ainsi la nature et l'envergure de la protection des données. L'existence parallèle de plusieurs réglementations pourrait être source de confusion. Les procédures qui ne sont pas encore pendantes ainsi que les dossiers de procédures closes sont en revanche soumis aux principes de la loi.

Article 5

Cette disposition énumère les principes de traitement les plus importants.

1er alinéa

Le traitement de données personnelles par des autorités, comme en principe toute autre activité de l'Etat, exige une base légale. Certains fichiers reposent sur des bases légales expresses (p.e. contrôle des habitants, registre foncier, registre du commerce ou des régimes matrimoniaux etc.), alors que d'autres sont créés pour servir à l'accomplissement d'une tâche définie par la loi. C'est lors de l'application de la loi qu'il conviendra d'apprécier et de décider au cas par cas si le traitement de données personnelles sert ou est nécessaire à l'accomplissement d'une tâche définie par la loi (cf. art. 3). L'accord de la personne intéressée ne remplace pas la base légale.

2e alinéa

C'est en premier lieu le but qui permet de juger de la licéité d'un traitement de données. Il n'est pas souhaitable que des données soient recueillies dans le seul but d'en constituer des réserves ou qu'elles soient à disposition pour des fins quelconques. Le but doit découler des bases légales ou des tâches que la loi assigne à l'autorité responsable.

3e alinéa

Même lorsque la base légale existe et que le but du traitement est déterminé, la loi autorise uniquement le traitement de données personnelles appropriées et nécessaires à l'accomplissement d'une tâche spécifique. L'administration publique tend à recueillir pour chaque cas particulier un très grand nombre de données afin d'obtenir un résultat qui soit le plus proche possible de la réalité. Là encore, il ne pourra être décidé qu'au cas par cas si un traitement de données personnelles répond ou ne répond pas à l'exigence de la proportionnalité.

4e alinéa

En limitant les possibilités d'abus, cette disposition a pour but de favoriser le climat de confiance qui règne entre citoyens et autorités et de promouvoir le traitement décentralisé des données personnelles. Les services administratifs ne sont autorisés à échanger des données personnelles ou à connecter des fichiers que si, selon le principe de la bonne foi, le citoyen doit s'y attendre. Certaines dispositions de la présente loi (p.e. art. 10, 2e al., art. 12, art. 15) ou de lois particulières (p.e. loi fiscale) sont réservées.

5e alinéa

Les dispositions sur la protection des données permettent notamment de concrétiser le secret de fonction et d'en définir les limites. Il n'est cependant pas exclu que certaines obligations particulières de garder le secret contenues dans des textes de lois spéciaux soient plus restrictifs que la présente loi.

Article 6

Lors du traitement de données particulièrement dignes de protection, ces conditions doivent venir s'ajouter à celles que prévoit l'article 5. Il est donc nécessaire qu'il y ait soit une base légale spécifique (et non seulement une base légale simple), cf. lettre *a*, soit une base légale simple au sens de l'article 5, 1er alinéa étayée par l'accord de la personne intéressée.

Article 7

Il est dans l'intérêt aussi bien du citoyen que des autorités que les données personnelles traitées soient exactes et complètes. La qualité des données sera cependant toujours relative. Il est donc nécessaire de prévoir une procédure de correction des données personnelles (art. 23). La présente disposition, qui est générale, oblige l'autorité qui traite des données, dans la mesure où l'on peut raisonnablement le lui demander, à s'assurer que les données soient correctes et complètes. De cette disposition peut également, si nécessaire, découler l'obligation de mentionner, lors de la transmission de données contestées, qu'il y a doute ou qu'il y a lieu de respecter une discrétion particulière. Le principe ancré dans cet article se relativise à mesure que le temps s'écoule: plus les recueils de données sont anciens, moins l'application du principe sera stricte.

Article 8

1er alinéa

Toute autorité qui, pour s'acquitter de la tâche que lui assigne la loi, traite ou fait traiter certaines données personnelles par un service indépendant (p.e. centre de calcul) est responsable de la protection des données au sens de la présente loi vis-à-vis de la personne intéressée.

2e alinéa

Il arrive fréquemment, en particulier lorsque le système de traitement des données est automatisé, que plusieurs autorités utilisent les données personnelles d'un seul et même fichier («banque de données»). Dans de tels cas, il convient de désigner une autorité qui assume la responsabilité principale de la protection des données. Cette disposition a pour but d'éviter que la personne intéressée soit renvoyée d'un service administratif à l'autre lorsqu'il y a usage commun de fichiers. Parallèlement, chaque autorité reste néanmoins responsable dans son domaine.

Article 9

Les principes généraux de traitement sont suivis de dispositions contenant des règles particulières, applicables à des modes de traitement spéciaux tels que l'acquisition et la transmission de données.

1er alinéa

En principe, l'administration doit recueillir les données dont elle a besoin non pas auprès de tiers mais auprès de l'intéressé lui-même. Les données devront en particulier par principe ne pas être recueillies auprès d'autres personnes de droit privé. Le terme «par principe» signifie que des exceptions sont possibles. Il convient en particulier de faire une exception lorsque le but en vue duquel les données ont été acquises ne peut pas être atteint autrement.

2e alinéa

En ce qui concerne l'acquisition de données à l'intérieur de l'administration, il convient d'attirer l'attention sur le fait que le citoyen n'aime pas se voir répéter les mêmes questions. L'administration peut donc se procurer des données auprès de ses propres services pour autant que la présente loi, en particulier l'article 5, 4e alinéa (respect de la destination des données) et l'article 5, 5e alinéa (obligations de garder le secret), ne s'y oppose pas.

3e et 4e alinéas

Les 3e et 4e alinéas règlent d'autres prétentions du citoyen dont il convient de tenir compte lors de l'acquisition de données. Le citoyen est ainsi en droit d'admettre que les autorités recueillent des données uniquement lorsqu'il est obligé de renseigner. Lorsque la loi ne prévoit pas de telle obligation, le caractère facultatif du renseignement doit être souligné. Le citoyen peut en outre exiger que lui soient communiqués la base légale et le but du traitement. Ces indications doivent figurer sur tous les questionnaires.

Article 10

1er alinéa

La communication de données personnelles est, du point de vue juridique, une étape particulièrement délicate du processus de traitement et exige de ce fait une réglementation détaillée. Il convient de rappeler ici que les conditions générales du traitement des données – donc aussi de leur communication (cf. art. 2, 3e et 4e al.) – figurent aux articles 5 et 6. La communication de données personnelles n'est admise que si ces conditions sont remplies. Deux situations sont alors envisageables: soit la communication de données fait partie des attributions de l'autorité qui renseigne (lettre *a*), soit l'autorité requérante a besoin de données. Dans le second cas, l'autorité requérante doit prouver qu'elle remplit les conditions exigées aux articles 5 et 6 (lettre *b*). L'autorité qui renseigne peut

exiger de telles preuves. Seule la comptabilité des buts (art. 5, 4e al.) n'est pas une condition impérative, cela uniquement, cependant, lorsque la communication sert les intérêts de la personne intéressée ou que celle-ci a donné son accord (lettre *c*).

2e alinéa

Les données du contrôle des habitants peuvent être communiquées à d'autres autorités à des *fins administratives*. Cela signifie que les conditions énumérées à l'article 5, 1er à 3e alinéas ainsi qu'à l'article 6 doivent néanmoins être remplies lors de la communication de données du contrôle des habitants, mais qu'en revanche la compatibilité des buts n'est pas indispensable. Cette concession est justifiée par le fait que le contrôle des habitants ne porte aucun jugement de valeur (cf. commentaire de l'art. 11) et que le citoyen pourrait souvent ne pas apprécier, en particulier lorsqu'il s'agit de ses données courantes, de devoir à chaque fois renseigner personnellement.

Article 11

Les auteurs du présent projet ont renoncé à créer une catégorie de «données libres» parce que le nom et l'adresse, en relation avec la tâche spécifique d'une autorité administrative, peuvent eux aussi représenter un intérêt digne de protection. Citons l'exemple d'un tiers qui voudrait savoir si le nom X figure dans les dossiers de tel pénitencier ou de telle maison d'éducation surveillée. Pour compenser l'absence de données libres, les auteurs de la présente loi n'ont pas opté pour une solution trop restrictive en ce qui concerne la communication de données à des particuliers par le contrôle des habitants, car ce dernier, contrairement à d'autres services administratifs, ne porte aucun jugement de valeur (cf. art. 12).

lettre *a*

La communication de données à des personnes de droit privé est autorisée – comme pour d'autres autorités – lorsque la loi l'impose ou l'autorise. Sont compris dans le terme de «loi» toutes les normes abstraites, quel que soit le niveau qu'elles occupent dans la législation, y compris p. e. une obligation de communiquer prévue dans une ordonnance d'exécution. Lorsqu'il s'agit de données personnelles particulièrement dignes de protection, des exigences plus strictes doivent être posées en ce qui concerne la base légale.

lettre *b*

Certaines données peuvent être communiquées si, non pas en général mais dans le cas d'espèce, un tel traitement sert manifestement les intérêts de la personne intéressée ou que celle-ci donne son accord exprès.

2e alinéa

Cette disposition sert à préciser que des données personnelles qui p. e. sont publiées dans une feuille officielle n'échappent pas complètement à la protection des données. Il est en particulier important que des données personnelles qui ont été ainsi publiées ne puissent pas être obtenues après avoir été classées selon de nouveaux critères ou jointes à d'autres indications publiées de quelque manière que ce soit.

3e alinéa

Cet alinéa tient compte du fait que certains ouvrages de référence, tels qu'annuaires d'adresses, listes de propriétaires de véhicules à moteur ou de bateaux et autres ouvrages de ce genre qui ont une certaine tradition et qui exigent que certaines données personnelles soient communiquées à des particuliers débordent le cadre de la présente loi. La communication de données personnelles aux éditeurs de ces publications devra être réglée au cas par cas par le Conseil-exécutif. Le livre des bourgeois de la commune bourgeoise de Berne rentre lui aussi dans cette catégorie de publications.

Article 12

Les tâches du contrôle des habitants revêtent un caractère général. Ce service administratif se prête par conséquent à l'exercice d'une fonction générale d'information, à l'intention des personnes et organisations de droit privé, qui manifestement répond à un besoin.

1er alinéa

Les données personnelles énumérées au 1er alinéa sont celles qui jouissent de la protection la plus faible. Le particulier peut obtenir de tels renseignements s'il en fait la demande oralement ou par écrit à la condition qu'il rende vraisemblable un intérêt justifié (qui ne doit donc pas forcément être un intérêt juridique). L'intérêt justifié ne constitue pas une condition très restrictive. Il s'agit en fait simplement d'éviter que les demandes présentées sans motif doivent être traitées. Etant donné le droit de blocage prévu à l'article 13, la fragilité de cette protection peut se justifier. Le 1er et le 2e alinéas régissent les requêtes que l'on pourrait qualifier de ponctuelles. Les requêtes par listes ne sont admises que si le règlement de commune le prévoit (3e al.).

2e alinéa

Plusieurs communes ont dans leurs règlements actuels assimilé les données énumérées au 2e alinéa à celles qui sont citées dans le premier. Il n'y a aucune raison impérative de ne pas laisser cette liberté aux communes (cf. introduction ci-devant, page 3 s.).

3e alinéa

Plusieurs communes prévoient la communication systématique de données personnelles, soit en général, soit pour des motifs idéaux. Etant donné le droit de blocage prévu, cette disposition est acceptable. Cela d'autant plus qu'une telle disposition du règlement doit être approuvée par les citoyens.

Article 13

Toute personne intéressée a le droit de faire bloquer ses données par l'autorité traitante, de sorte qu'elles ne soient pas communiquées à des personnes ou organisations de droit privé. Ce droit de blocage s'applique sans conditions aux données au sens de l'article 12, 2e et 3e alinéas. L'expérience pratique démontre que les demandes de blocage sont rares. Dans tous les autres cas, la communication de données à des particuliers peut être bloquée si la personne intéressée prouve un intérêt digne de protection. Citons l'exemple de femmes vivant séparées de leur mari qui craignent que ces derniers veuillent reprendre leurs enfants dont elles ont obtenu la garde ou l'exemple de réfugiés politiques qui se sentent menacés par des agents étrangers.
Il s'agit là d'une limitation du droit de blocage. D'une part, ce droit ne doit entraver ni l'accomplissement de la tâche définie par la loi ni l'obligation légale de renseigner. D'autre part, l'exercice abusif de ce droit ne doit jouir d'aucune protection. Si p.e. la créancière d'une contribution d'entretien rend vraisemblable auprès du contrôle des habitants que le débiteur n'a demandé le blocage que pour échapper à la poursuite, l'adresse du débiteur pourra lui être communiquée malgré l'ordre de blocage.

Article 14

1er alinéa

Cette disposition s'applique non seulement à la communication de données à des autorités ou à des particuliers, mais également à la communication de données par le contrôle des habitants. Cet alinéa permet, dans le cas concret, de restreindre encore la communication de données personnelles, telle que la règlent les articles précités, lorsque des intérêts publics majeurs ou des intérêts privés particulièrement dignes de protection l'exigent. Tel peut notamment être le cas lors de travaux de planification ou de recherche dans le domaine militaire ou lors du traitement de données sensibles concernant une personne en détention pénale.

2e alinéa

Outre la réserve générale que constitue le secret de fonction, le 2e alinéa mentionne les prescriptions particulières imposant le secret, telles qu'elles existent p.e. dans le domaine de la santé. Les données personnelles qui jouissent d'une telle protection ne peuvent être communiquées que si le requérant (autorité ou personne de droit privé) est soumis à une telle obligation de garder le secret.

Article 15

1er alinéa

Le traitement de données personnelles pour les besoins de la statistique, de la planification ou de la recherche scientifique jouit de conditions beaucoup plus souples en matière de protection des données parce que la personne intéressée ne compte en l'occurrence pas en tant qu'individu mais uniquement en tant qu'unité statistique anonyme. Le présent alinéa exige toutefois que, dès que le but du traitement le permet, les données personnelles soient rendues anonymes et que les résultats soient publiés sans références personnelles.

2e alinéa

L'autorité responsable est autorisée à communiquer des données personnelles à d'autres autorités ou personnes de droit privé qui désirent les traiter sans référence aux personnes intéressées si le destinataire garantit la sécurité des données et ne les transmet pas à un tiers. La convention écrite est probablement le meilleur moyen de s'assurer de cette garantie supplémentaire. Le destinataire devra dans tous les cas transformer dès que possible les données personnelles en données anonymes et publier les résultats sans faire référence aux personnes intéressées.

Article 16

Le mandat de traitement fait du mandataire une autorité au sens de l'article 2, 5e alinéa, avec toutes les responsabilités que cette qualité implique. Vis-à-vis du citoyen toutefois, le mandant continuera à être le principal responsable de la protection des données (art. 8, 2e al.).

Article 17

Cela veut dire que l'autorité qui traite des données est responsable de leur sécurité. Elle devra s'organiser en conséquence et prendre à cet effet toutes les mesures techniques et administratives appropriées. Elle devra en particulier protéger les données contre
- le vol et la communication à des personnes non autorisées;
- les dommages, les modifications, l'immixtion de tiers et la destruction involontaire;
- les variations de température néfastes, l'humidité, l'influence de champs magnétiques;
- les erreurs de traitement et de manipulation et les conséquences de pannes de systèmes.

Article 18

Le nombre croissant des tâches de l'administration et les moyens techniques qu'elle utilise pour s'en acquitter ont compliqué sa structure et ses activités d'information à tel point que bon nombre de ses domaines échappent aujourd'hui à

la compréhension du citoyen. Il est donc capital pour l'efficacité d'une loi sur la protection des données, qui vise à renforcer la position et la confiance du citoyen face à l'administration, de révéler les sources et les flots d'informations dont dispose l'administration. Le citoyen doit donc fondamentalement avoir la possibilité de savoir quels sont les services qui traitent des données, de connaître la nature des données, le but du traitement et le nom des personnes qui ont accès aux données afin de pouvoir, en cas de besoin, faire valoir ses droits d'accès, de correction, de destruction etc. dont il jouit auprès de l'autorité responsable aux termes du présent projet de loi. Un registre contenant de telles informations revêt une fonction de marche à suivre pour le citoyen. Pour l'administration elle-même, il peut en outre représenter un instrument très utile favorisant l'ordre et la rationalisation. Le registre, géré par l'autorité de surveillance, est public (art. 20).

2e alinéa

L'inscription des fichiers se fera le plus rationnellement au moyen d'un formulaire unique élaboré à l'intention du canton ou des communes, qui comportera les rubriques énumérées au 2e alinéa.

lettre *a*

Doit être indiquée soit la base légale, soit la tâche définie par la loi qu'il est prévu de remplir à l'aide du fichier.

lettre *b*

Lorsqu'il y a plusieurs autorités responsables, elles doivent être nommées en plus de l'autorité qui assume la responsabilité principale (art. 8).

lettre *c*

Pour ce qui est des moyens mis en œuvre, il convient en particulier d'indiquer si le traitement du fichier est électronique ou conventionnel.

3e alinéa

La tenue du registre ne doit pas demander un travail administratif trop important. Etant donné la multitude de fichiers dont dispose l'administration publique, il convient de restreindre l'obligation d'enregistrement.

lettre *a*

Cette disposition concerne les fichiers qui sont appelés à disparaître rapidement (fichier constitué p. e. pour quelques semaines seulement dans un but bien précis).

lettre *b*

Il s'agit là p. e. de l'annuaire officiel ou de listes électorales.

3e alinéa, dernière phrase

Ces fichiers doivent être déclarés à l'autorité de surveillance, mais ne sont pas inscrits au registre public. Les fichiers qui ne sont ni enregistrés ni déclarés sont interdits.

Article 19

L'idée que les données personnelles traitées ne seront un jour plus utilisées ou deviendront superflues et qu'elles devront donc être détruites ou radiées n'est guère familière à l'administration publique, qui a tendance à conserver pour des durées illimitées tous les recueils de données. Pourtant, l'avalanche d'informations qui nous ensevelit actuellement nous oblige régulièrement à éliminer certains dossiers et systèmes d'information. Cette situation exige que la date de destruction des données personnelles soit fixée pour chaque fichier. La durée de conservation sera le plus souvent fixée à 10 ou 15 ans. Les conditions qui peuvent justifier une conservation au delà de cette date sont énumérées au 3e alinéa, les dispositions applicables aux archives publiques (RSB 421.21) sont quant à elles réservées. Cette disposition, formulée ici de façon assez simple est un moyen judicieux d'amorcer un projet à long terme, qui va soulever quelques problèmes complexes.

Article 20

Le registre est donc public.

Article 21

1er alinéa

La garantie du droit d'accès aux données relatives à sa propre personne est un objectif majeur de la loi sur la protection des données. L'autorité responsable renseigne en principe uniquement au sujet des données personnelles qui concernent le requérant et qui figurent dans un fichier déterminé. Contrairement à ce que pensent de nombreuses personnes, les services administratifs ne sont souvent pas à même – et doivent ne pas l'être – d'indiquer à la personne intéressée les autres fichiers qui contiennent des données la concernant, car les connections de fichiers qui y seraient nécessaires n'existent pas et seraient d'ailleurs interdites (p. e. en raison de l'art. 5, 4e al.). Un tiers peut être renseigné uniquement en vertu des dispositions du droit administratif général, c'est-à-dire en sa qualité de représentant légal ou de représentant par procuration. Etant donné que le droit d'accès sert à protéger la personnalité, il ne peut fondamentalement pas être dénié au mineur capable de discernement. Le requérant devra justifier de son identité. Un renseignement peut en outre être donné à un tiers si les conditions des articles 10 ss. sont remplies.

2e alinéa

Nul ne peut renoncer à son droit d'accès.

3e alinéa

Le renseignement peut être demandé oralement ou par écrit. L'autorité responsable doit toutefois s'assurer que le requérant est en droit de demander le renseignement, ce qui p.e. est en règle générale impossible pour les demandes téléphoniques. L'obligation de donner le renseignement sous une forme généralement compréhensible a pour but d'éviter que la personne intéressée se voit répondre au moyen de termes techniques compliqués ou de codes TED. Un renseignement écrit peut p.e. être nécessaire pour étayer son propre droit à se défendre.

4e alinéa

La personne intéressée peut aussi exercer son droit d'accès en consultant les données. Ce mode de renseignement peut cependant être refusé pour des raisons importantes, lorsque p.e. les dossiers sont volumineux et contiennent, outre les données relatives au requérant, des données personnelles concernant des tiers qui ne peuvent pas être simplement dissimulées. Dans ce cas, le requérant devra se contenter d'un renseignement au sens du 1er alinéa.

5e alinéa

Cette disposition a pour but d'épargner aux autorités des requêtes fréquentes et totalement injustifiées.

Article 22

1er alinéa

Toute restriction du droit d'accès ne doit pas seulement découler de la structure du fichier ou du traitement, comme à l'article 21, 4e alinéa, mais doit avoir des raisons matérielles, qui s'opposent à ce qu'un renseignement soit fourni au requérant. Le public pourrait p.e. avoir un intérêt à ce qu'un secret en matière de protection civile soit gardé. La personne intéressée ne pourra pas se renseigner directement sur les données contenues dans les fichiers de la police, raison pour laquelle l'autorité de surveillance doit défendre les intérêts des citoyens (art. 30). Les procédures pénales pendantes sont réservées. Dans ces cas, le droit d'accès est régi par les règles de la procédure pénale (art. 4, 2e al., lettre *c*).

2e alinéa

Cette restriction du droit d'accès a été introduite pour protéger la personnalité de l'intéressé même. Dans le domaine de la santé, notamment, il est des renseignements qui seraient trop affligeants pour la personne intéressée et qu'il vaut donc mieux donner à une personne jouissant de sa confiance. Les dispositions du 2e alinéa doivent être appliquées avec beaucoup de retenue.

3e alinéa

Les dispositions qui précèdent n'empêchent pas qu'un renseignement soit demandé par pure curiosité. Pour des raisons financières, il ne doit toutefois pas en résulter un travail administratif trop important. Le travail, même important, doit être accepté dans tous les cas où le requérant rend au moins vraisemblable un intérêt digne de protection.

Article 23

1er alinéa

Toute donnée inexacte doit être corrigée et toute donnée inutile doit être détruite (cf. également art. 7 et 19).

2e alinéa

En principe, c'est à l'autorité responsable qu'incombe le fardeau de la preuve. Toutefois, dans la mesure où l'on peut raisonnablement le lui demander, la personne intéressée doit contribuer à clarifier la situation.

3e alinéa

Il faut aussi prévoir le cas où ni l'exactitude ni l'inexactitude ne peuvent être prouvées irréfutablement. Tel sera notamment le cas des jugements de valeur, qui sont, il est vrai, nécessaires – p.e. pour qualifier des collaborateurs – mais qui ne peuvent pas être prouvés de façon claire et nette. Dans de tels cas, il conviendra de tenir dûment compte de l'optique de la personne intéressée.

Article 24

1er alinéa

Outre le droit de contrôler l'exactitude de ses données, la personne intéressée peut en interdire le traitement si p.e. la base légale fait défaut, s'il est disproportionné ou si son but est incompatible avec le but originel du traitement (cf. art. 5 ci-devant).
Toute donnée personnelle traitée de façon illicite doit être détruite ou alors les effets du traitement illicite doivent être éliminés.

2e alinéa

Cette prétention comprend également le droit à la publication, pour autant qu'il existe un intérêt digne de protection.

Article 25

1er alinéa

Les personnes de droit public ont donc une responsabilité causale. Cette disposition correspond à celle que l'on retrouve dans la loi-modèle et dans le projet

de loi fédérale. Elle va plus loin que la responsabilité civile générale des fonctionnaires de l'Etat (art. 38 de la loi sur les fonctionnaires; RSB 153.01). La loi sur les communes prévoit une responsabilité causale des communes pour tout dommage causé illicitement par leurs fonctionnaires (art. 38 de la loi sur les communes; RSB 170.1). Là encore les organisations et personnes de droit privé chargées de tâches publiques sont assimilées aux autorités communales (art. 2, 5e al.). Les litiges de ce genre relèvent du droit public.

2e alinéa

Dans des circonstances graves, la personne lésée a droit à réparation.

3e alinéa

Lorsque l'autorité, l'organe, le fonctionnaire, l'employé ou le mandataire a agi intentionnellement ou s'est rendu coupable d'une négligence grave, un droit récursoire est prévu. Peuvent faire usage de ce droit l'Etat, les communes, les corporations, les institutions ou les personnes de droit privé qui ont dû verser des dommages-intérêts et donner réparation à la personne lésée.

Article 26

Cela signifie que les décisions concernant la protection des données peuvent être attaquées par les voies de recours ordinaires. Ce n'est par conséquent pas l'autorité de surveillance qui est autorité de recours mais les autorités de justice administrative qui tranchent également des recours ayant trait à d'autres domaines.

Article 27

Les autorités de surveillance ne sont pratiquement autorisées à arrêter des décisions qu'en rapport avec des enregistrements.

Article 28

Il n'est pas certain qu'une ordonnance formelle relative à une requête au sens des articles 21 à 24 réunisse tous les éléments d'une décision. La présente disposition vise à établir clairement que de telles ordonnances, ou le fait de les refuser ou de les différer, sont elles aussi attaquables.

Article 29

Si une autorité demande à une autre autorité de lui communiquer des données personnelles et que celle-ci lui refuse le renseignement, l'autorité qui a été déboutée doit pouvoir se défendre lorsque, conformément à la présente loi, elle a le droit d'obtenir cette information.

Article 30

En vertu des règles proposées ici, les fichiers de police doivent être enregistrés. Le registre doit contenir les indications mentionnées à l'article 18, 2e alinéa. Le particulier quant à lui n'a aucun droit d'y accéder. S'il veut faire contrôler l'exactitude de ses données personnelles qui sont fichées par la police, il peut déposer une requête au sens des articles 21 à 24 auprès de l'autorité de surveillance (cf. art. 34, lettre *f*). Celle-ci défend les intérêts de la personne intéressée et lui fait part des résultats de ses démarches. Dans ce cas, l'autorité de surveillance a les mêmes droits que l'intéressé lui-même. Si nécessaire, elle peut p. e. recourir au nom de la personne intéressée.
Dans la mesure où la police agit en application de l'article 17, 3e alinéa de la loi fédérale sur la procédure pénale, elle est soumise aux dispositions du droit fédéral. L'application de la loi cantonale est exclue dans ce domaine. En fait, la Confédération a, pour l'instant, émis des prescriptions régissant certains aspects de la question. L'élaboration d'autres directives est prévue d'ici à ce que l'ensemble de la matière soit réglé dans la loi fédérale sur la protection des données personnelles (art. 58).

Article 31

1er alinéa

Correspond dans les grandes lignes aux dispositions des articles 46 ss. de la loi sur les finances de l'Etat (RSB 621).

Article 32

L'autorité de surveillance a une fonction importante pour l'application de la loi sur la protection des données. Elle n'est, il est vrai, pas une instance de recours – les recours seront adressés aux instances habituelles au sens de l'article 26 – mais remplit sa tâche de surveillance en tant qu'intermédiaire entre les personnes intéressés et les autorités traitantes ou responsables (cf. art. 34). Elle doit avoir les connaissances spéciales nécessaires et avoir une certaine autorité interne. Raison pour laquelle il est prévu qu'elle soit élue par le Grand Conseil. Quant à savoir si la surveillance devait être assumée par une commission ou par un délégué, le groupe de travail chargé d'élaborer le projet était divisé. Une majorité s'est toutefois prononcée en faveur d'une commission, comme l'ont fait les auteurs de la loi-modèle et du projet de loi fédérale. Le Conseil-exécutif partage quant à lui cet avis. Une commission de cinq membres (probablement 3 députés au Grand Conseil et deux experts, p. e. un informaticien et un juriste fonctionnaires ou non de l'administration) garantit les connaissances spéciales nécessaires ainsi qu'une certaine autorité. Elle pourra se réunir en cas de nécessité. Son président, appuyé par le secrétariat, se charge des affaires courantes et prépare les séances. La majorité des membres du groupe de travail a estimé que cette solution est moins coûteuse et mieux adaptée à la structure des autorités bernoises que la désignation d'un délégué pour la protection des données.

Cette solution d'un délégué unique personnifierait plus l'autorité de surveillance qui alors pourrait être d'un accès plus facile pour la population. Pour la Commission, c'est le président (connu par le public) qui devrait assumer cette fonction de point de contact. Le choix du délégué présenterait un autre avantage: il pourrait agir plus librement. Mais, désavantage, il faudrait alors créer un nouveau poste, payer un salaire qui corresponde à l'autorité requise et mettre un secrétariat à la disposition du délégué (coût annuel env. 100000 à 150000 fr.). Enfin le volume de travail serait vraisemblablement très variable, élément qui parle également en faveur d'une commission assistée d'un secrétariat tenu par un service administratif existant, celui-ci pouvant en effet réagir avec souplesse face au volume de travail à effectuer. Le secrétariat peut être rattaché à la Direction de la justice, compétente en matière de protection des données. Si un délégué à la protection des données est désigné, il faudrait mettre à sa disposition le personnel de secrétariat nécessaire. L'intégrer à une structure administrative existante serait pratiquement impossible.

Article 33

La formulation neutre «autorité de surveillance» laisse aux communes la possibilité d'adopter des réglementations diverses. Elles peuvent opter en faveur soit d'une commission, soit d'un délégué à la protection des données.

Article 34

lettre *a*

Voir article 18.

lettre *b*

Voir article 35.

lettre *f*

Voir articles 22 et 30. L'autorité de surveillance a les mêmes prérogatives que les particuliers. Elle peut, le cas échéant, faire usage des moyens de recours.

Article 35

L'autorité de surveillance a besoin non seulement d'une certaine indépendance, mais aussi de garanties légales qui lui permettent de faire son travail en toute liberté; sinon elle n'aurait aucune crédibilité aux yeux du citoyen et elle n'aurait plus guère d'utilité pour les autorités politiques. Les examens auxquels doivent procéder les membres et les collaborateurs de l'autorité de surveillance exigent naturellement de leur part certaines connaissances sur la technique et le droit, ainsi que sur l'appareil administratif.

Article 36

Le droit qu'a l'autorité de surveillance d'exiger des renseignements, en dépit d'éventuelles obligations de garder le secret, auprès d'autorités (art. 35, 2e et 3e al.) exige que l'autorité de surveillance soit soumise à la même obligation de garder le secret que l'autorité traitante.

2e alinéa

Lorsqu'il ne s'agit pas d'informations fournies par d'autres autorités ou des tiers, les membres de l'organe de surveillance sont tenus au secret en vertu de l'article 36, 2e alinéa.

Article 38

Cette disposition confère au Conseil-exécutif le pouvoir d'édicter les dispositions d'exécution nécessaires. Elle souligne également que le Conseil-exécutif a la possibilité de créer une base légale précise au sens de l'article 6, lettre *a*.

Article 39

La 2e phrase doit permettre, si nécessaire, de tenir compte du postulat Haudenschild.

Berne, le 26 juin 1985

Le directeur de la justice: *Schmid*