Proposition commune du Conseil-exécutif et de la commission

Loi sur la protection des données (LCPD) (Modification)

Direction de la justice, des affaires communales et des affaires ecclésiastiques

Rapport
présenté par le Conseil-exécutif au Grand Conseil concernant la modification de la loi sur la protection des données

1. Situation initiale

1.1 Droit sur la protection des données en vigueur

La protection des données concerne un domaine central de la personnalité de l'être humain. Elle fait partie de la protection de la sphère privée[1)] garantie par l'article 13 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.)[2)]. L'article 13, alinéa 2 Cst. prévoit expressément à cet égard une protection contre l'emploi abusif des données personnelles. La Constitution du canton de Berne du 6 juin 1993 (Constitution cantonale, ConstC)[3)] comprend à l'article 18 une garantie complète relative à la protection des données.

En matière de protection des données, tant la Confédération que les cantons disposent de compétences législatives. La Confédération règle par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[4)] le traitement des données par des personnes privées et des organes fédéraux. Les cantons, quant à eux, sont compétents pour réglementer le traitement de données par des organes cantonaux et communaux. Le canton de Berne dispose, avec la loi cantonale du 19 février 1986 sur la protection des données (LCPD)[5)], d'un droit qui peut, aujourd'hui encore, être considéré comme adapté aux conditions actuelles et dont l'application a, dans l'ensemble, donné satisfaction.

1.2 Droit de l'Union européenne

Le 26 octobre 2004, les Chambres fédérales ont approuvé les accords sectoriels bilatéraux avec l'Union européenne (UE) sur les produits agricoles transformés, la statistique, l'environnement, les programmes MEDIA, les pensions, Schengen/Dublin, la lutte contre la fraude et la fiscalité de l'épargne (dits «Bilatérales II»)[6)]. Suite à l'aboutissement d'un référendum, le peuple suisse a voté le 5 juin 2005 en faveur de l'accord d'association à Schengen/Dublin, dont l'objet est de favoriser une collaboration étroite de la Suisse avec l'UE dans les domaines de la police, de la justice et de l'asile. Le Système d'information Schengen (SIS), véritable clé de voûte de la coopération dans le domaine de la police, est une plateforme de dimension européenne qui permet d'échanger des informations portant sur les recherches policières. Consciente du fait que de tels systèmes portent également gravement atteinte aux droits de la personnalité des personnes concernées, l'UE a parallèlement édicté des règles strictes sur la protection des données que la Suisse se doit aujourd'hui également de respecter en raison de son association à Schengen/Dublin.

L'application, dans le détail, de telle ou telle réglementation dépend du «pilier» auquel le domaine en question appartient. Avec le Traité d'Amsterdam, les actes législatifs et les mesures constituant l'acquis de Schengen ont été intégrés dans l'édifice juridique de l'UE qui, depuis le Traité de Maastricht, comporte trois piliers: le premier est formé par la CE (Traité instituant la Communauté européenne, TCE), le deuxième comprend les dispositions concernant la politique étrangère et de sécurité commune et le troisième regroupe les dispositions relatives à la coopération policière et judiciaire en matière pénale. Dans cet acquis de Schengen, les prescriptions relatives à la protection des données que la Confédération doit reprendre en s'associant à Schengen/Dublin sont décrites de manière détaillée. A cet égard, les documents suivants sont importants: la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[7)] (directive de l'UE sur la protection des données, ci-après «directive de l'UE»), la Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[8)] (Convention) et le Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données[9)] (Protocole additionnel), que les Chambres fédérales ont adopté le 24 mars 2006 en même temps que la révision de la loi fédérale sur la protection des données[10)].

1.3 Application des prescriptions européennes

L'accord bilatéral sur l'association à Schengen/Dublin se rapporte aussi bien à des domaines qui relèvent de la compétence de la Confédération qu'à ceux qui ressortissent aux cantons ou dont l'exécution incombe tout au moins à ces derniers. Par conséquent, la Confédération, mais aussi les cantons sont responsables de l'application des accords. La Confédération a tenu compte des prescriptions européennes dans le cadre de la révision du 24 mars 2006 de la loi sur la protection des données.

1) Contrairement au droit européen, le droit suisse sur la protection des données protège non seulement les personnes physiques mais également les personnes morales.
2) RS 101
3) RSB 101.1
4) RS 235.1
5) RSB 152.04
6) Cf. à ce sujet le message du Conseil fédéral relatif à l'approbation des accords bilatéraux entre la Suisse et l'Union européenne, y compris les actes législatifs relatifs à la transposition des accords («Accords bilatéraux II») du 1er octobre 2004, FF 2004, p. 5593 ss.
7) Journal officiel des Communautés européennes n° L 281 du 23 novembre 1995, p. 0031 à 0050
8) RS 0.235.1
9) FF 2003, p. 1977 ss
10) FF 2006, p. 3421

En vue de la mise en œuvre des prescriptions légales européennes portant sur la protection des données, la Conférence des gouvernements cantonaux (CdC) a fait rédiger le guide pratique intitulé «Mise en œuvre Schengen/Dublin dans les cantons: protection des données» daté du 15 mars 2006 (ci-après «guide de la CdC»). Celui-ci se compose d'une liste de contrôle (check-list) et de commentaires relatifs à chaque rubrique. Ce guide doit permettre aux cantons de vérifier dans quelle mesure leur législation sur la protection des données correspond aux exigences européennes et dans quel domaine il convient encore d'agir ou de réglementer.

Le guide de la CdC a également servi de base aux travaux préparatoires de la révision de la loi cantonale sur la protection des données. Se fondant sur des études préliminaires, le Conseil-exécutif a chargé la Direction de la justice, des affaires communales et des affaires ecclésiastiques (JCE), le 28 juin 2006, de vérifier dans quelle mesure le droit cantonal devait être adapté et de présenter des propositions à ce sujet. L'organisation de projet mise en place par la JCE a livré le 28 novembre 2006 un rapport intermédiaire au Conseil-exécutif. Le présent projet se fonde sur le guide de la CdC, les résultats exposés par le rapport intermédiaire de l'organisation de projet et les décisions du Conseil-exécutif concernant certaines propositions et recommandations de cette organisation.

En 2007 et en 2008, l'UE va vérifier, dans le cadre d'une évaluation effectuée à deux niveaux, si la législation suisse, tant fédérale que cantonale, répond à la norme de Schengen. La mise en œuvre pratique fera ensuite l'objet d'un examen sur place.

1.4 Objectifs et lignes directrices de la révision

La révision s'est basée sur les lignes directrices et les objectifs suivants:

- Le principal objectif consiste à créer une législation bernoise en matière de protection des données qui soit juridiquement eurocompatible. A cet égard, le droit cantonal doit être conçu de telle sorte que les contrôles que l'UE effectuera en 2007 et en 2008 ne révèlent aucun point pouvant constituer un obstacle à l'entrée en vigueur des accords de Schengen et de Dublin.
- Les prescriptions du droit européen doivent également être mises en œuvre de façon pragmatique. La révision doit se limiter à des adaptations qui, du fait de ces prescriptions ou pour d'autres motifs, semblent indispensables. Là où une adaptation s'avère nécessaire, les nouveautés doivent dans la mesure du possible s'intégrer à l'ensemble des réglementations actuelles qui ont fait leurs preuves et concorder également avec les prescriptions choisies par la Confédération dans le cadre de la mise en œuvre du droit de l'UE pour autant que des spécificités concrètes du canton de Berne n'exigent pas l'adoption de dispositions divergentes.

2. Les grandes lignes du projet

2.1 Aperçu des adaptations nécessaires

L'examen du droit en vigueur à la lumière des prescriptions européennes et du guide de la CdC a montré que les adaptations nécessaires concernent avant tout le statut juridique de la surveillance de la protection des données et les compétences de l'autorité de surveillance. Il est demandé a priori que la loi précise que l'autorité de surveillance travaille «en toute indépendance» et qu'elle garantisse celle-ci par des dispositions relevant de l'organisation (élection/désignation et statut juridique des personnes responsables de la surveillance, mise à disposition de ressources, statut de l'autorité au sein de la structure étatique). Au vu des compétences de l'autorité de surveillance, les tâches et les pouvoirs qui lui reviennent, ainsi que les instruments dont elle a besoin pour les gérer efficacement devront faire partiellement l'objet de nouvelles réglementations.

Au surplus, les prescriptions européennes exigent uniquement des réglementations ou des adaptations ponctuelles, notamment en ce qui concerne la validité des dispositions du droit sur la protection des données dans les procédures administratives pendantes, les coûts pour la consultation de données et la demande de renseignements ainsi que les flux transfrontières de données. Les adaptations exigées par l'association de la Suisse à Schengen/Dublin offrent l'occasion de proposer une nouvelle réglementation partielle des registres en matière de protection des données, d'introduire la question du rapport que l'autorité de surveillance doit soumettre, mais aussi de biffer une disposition dont l'application pratique n'a jamais été requise (art. 27 LCPD, recours contre l'autorité de surveillance) et d'apporter une précision au sujet de la procédure et de la protection juridique.

2.2 Adaptations ponctuelles de la loi sur la protection des données

2.2.1 Champ d'application de la loi

Selon la réglementation en vigueur, la loi sur la protection des données n'est pas applicable aux procédures civiles, administratives ou pénales qui sont pendantes ni aux recherches effectuées par les commissions d'enquête parlementaires (art. 4, al. 2, lit. *c* LCPD). La procédure administrative préalable au prononcé d'une décision est également exclue du champ d'application de la loi[11]. L'article 4, alinéa 2, lettre *c* LCPD devait tenir compte du fait qu'il existe pour les procédures précitées des lois particulières, à savoir le Code de procédure civile du 7 juillet 1918 (CPC)[12], la loi du 23 mai 1989 sur la procédure et la juridiction administratives (LPJA)[13] et le Code de procédure pénale du 15 mars 1995 (CPP)[14], qui traitent la question des données de manière indépendante. Il s'agissait d'éviter la coexistence de deux réglementations qui poursuivent pour l'essentiel le même but de protection.

Selon le guide de la CdC, la procédure administrative ne peut en aucun cas être exclue du champ d'application des lois cantonales sur la protection des données. Une adaptation du champ d'application dans ce domaine également s'avère indiquée. Ainsi, l'autorité de surveillance de la protection des données peut, dans ce cas

[11] Jugement du Tribunal administratif du canton de Berne n°18226 du 26 août 1991 in JAB 1992, p. 80 ss
[12] RSB 271.1
[13] RSB 155.21
[14] RSB 321.1

seulement, faire usage de ses compétences dans une procédure préalable au prononcé d'une décision également, par exemple dans le cadre d'une taxation fiscale (cf. ch. 2.4 infra). Par ailleurs, dans le cadre de l'exécution du droit fédéral, la loi fédérale sur la protection des données s'applique également à des procédures administratives de première instance lorsqu'une autorité cantonale est compétente en matière d'exécution (art. 2, al. 2, lit. *c* en relation avec l'art. 37, al. 1 LPD). Une adaptation de la loi cantonale sur la protection des données permet d'éviter que la validité de la protection des données dépende du fait que l'exécution du droit fédéral soit ou ne soit pas également concernée. Il n'est pas possible de séparer clairement ces deux cas dans le cadre du contrôle préalable nouvellement introduit (cf. infra ch. 2.4.2 et 3.1, commentaire relatif à l'art. 17a). Si le champ d'application actuel de la loi cantonale sur la protection des données était maintenu, des problèmes pratiquement insolubles se présenteraient.

D'après le guide de la CdC, il serait également délicat que la procédure de recours administratif interne ne soit pas soumise au champ d'application de la loi sur la protection des données. Le guide motive cela uniquement en se référant à la réglementation de droit fédéral prévue à l'article 2, alinéa 2, lettre *c* LPD selon laquelle le droit de la Confédération en matière de protection des données s'applique uniquement aux procédures administratives, et non aux procédures de justice administrative. Une adaptation pragmatique du droit de la protection des données s'inspirant du droit fédéral devrait par conséquent passer par une modification de l'article 4, alinéa 2 LCPD, n'allant pas au-delà toutefois de ce que prévoit la loi fédérale. Il faut donc que les procédures administratives préalables au prononcé d'une décision soient désormais soumises au champ d'application de la loi cantonale. On peut ainsi partir du principe que lors de procédures de recours formelles, la protection des données et les droits des personnes intéressées sont suffisamment garantis par les dispositions applicables de la loi sur la procédure et la juridiction administratives.

L'extension du champ d'application ne signifie pas que la loi cantonale sur la protection des données supplante automatiquement, dans tous les cas, les dispositions de la loi sur la procédure et la juridiction administratives. Dans un cas concret, lors de dispositions en concurrence, il conviendra d'examiner, au moyen de critères d'interprétation d'actes législatifs reconnus (p. ex. prééminence de la *lex specialis*) laquelle d'entre elles s'applique en priorité. Il semble que jusqu'à maintenant, l'utilisation simultanée de dispositions de droit de la protection des données et de droit procédural par la Confédération n'ait donné lieu à aucun problème notable dans le cadre de l'application du droit.

2.2.2 Coûts pour la demande de renseignements et la consultation de fichiers

Le droit d'obtenir des renseignements sur des données personnelles et de consulter des fichiers est un élément essentiel de la protection de la personnalité prévue par la Constitution (art. 18, al. 1 ConstC). L'article 12, lettre *a* de la directive de l'UE prévoit par conséquent que toute personne intéressée doit pouvoir obtenir des renseignements sans frais excessifs et sans que ses recherches ne soient rendues plus difficiles ou même contrecarrées. Par conséquent, il convient d'inscrire clairement dans la loi que la consultation de fichiers ou la demande de renseignements est en principe gratuite et qu'un émolument ne peut être perçu qu'à titre exceptionnel.

2.2.3 Flux transfrontières de données

Selon l'article 2, chiffre 1 du Protocole additionnel, le flux transfrontières de données n'est admissible que si l'Etat destinataire «assure un niveau de protection adéquat pour le transfert considéré» (cf. aussi l'art. 12 de la Convention et des art. 25 s. de la directive de l'UE). Selon l'article 2, chiffre 2 du Protocole additionnel, les dérogations à ce principe doivent être réglementées légalement. Cette disposition entraîne par ailleurs une obligation d'informer l'autorité de surveillance de la protection des données.

Jusqu'à maintenant, le canton de Berne n'a guère dû se préoccuper de flux de données avec l'étranger, raison pour laquelle ce cas n'est d'ailleurs pas réglementé dans le droit en vigueur. La clause générale portant sur l'ordre public prévue à l'article 14, alinéa 1 LCPD s'avère insuffisante, au vu des prescriptions de droit européen mentionnées, pour réglementer les flux transfrontières de données car la spécificité exigée lui fait défaut. Une réglementation s'inspirant de l'article 2 du Protocole additionnel doit donc être intégrée à la loi. Etant donné que la Confédération a tenu compte du Protocole additionnel en procédant à la révision de sa loi sur la protection des données, il est conseillé de se fonder sur cette dernière pour adapter la loi cantonale.

2.2.4 Registre des fichiers

L'enregistrement des fichiers aide les personnes intéressées à faire valoir leurs droits, notamment le droit à l'obtention de renseignements et à la consultation des données (art. 21 LCPD), le droit à la rectification ou à la destruction de données personnelles les concernant qui ne sont pas exactes ou pas nécessaires (art. 23 LCPD) et le droit au blocage (art. 13 LCPD). La loi sur la protection des données et l'article 21, alinéa 2 de la directive de l'UE prévoient donc que tous les fichiers doivent être inscrits dans un registre. Selon la directive de l'UE, le registre doit être tenu par l'autorité de contrôle. Dans le canton de Berne également, c'est à l'heure actuelle l'autorité de surveillance qui tient à jour le registre des fichiers (art. 34, lit. *a* LCPD). L'autorité responsable annonce chaque fichier à son autorité de surveillance, qui les enregistre (art. 18 LCPD).

Dans la pratique, l'établissement et surtout la mise à jour d'un registre central des fichiers soulève des difficultés importantes, car seul l'organe responsable du traitement des données, et non l'autorité de surveillance, sait quels sont les fichiers qui existent, qui sont nouvellement établis ou détruits. Il paraît donc approprié de réglementer l'enregistrement sous une forme partiellement nouvelle. Etant donné que selon l'article 21, alinéa 2 de la directive de l'UE, il revient expressément à l'autorité de contrôle de tenir le registre, une décentralisation complète prévoyant que seuls les organes traitant les données enregistrent les fichiers dont ils disposent ne serait pas admissible. La solution prônant que l'autorité de surveillance tient un registre

central qui, selon les prescriptions de cette dernière, est «géré», c'est-à-dire établi et, si nécessaire, mis à jour par les autorités responsables, paraît judicieuse et se révèle en outre compatible avec la directive de l'UE. Grâce à une telle solution, les personnes intéressées peuvent se renseigner en un seul lieu sur l'ensemble des fichiers constitués dans le canton ou dans une collectivité de droit communal. L'autorité de surveillance devra s'assurer, par des prescriptions adaptées, de l'enregistrement effectif des fichiers.

2.2.5 Procédure et protection juridique

Lors de mesures relevant du droit de la protection des données, le droit en vigueur prévoit généralement à leur encontre, de manière non exclusive, les moyens de droit ou les moyens non juridictionnels auprès des autorités de justice administrative, mais aussi, dans certains cas, des autorités de justice civile ou pénale (cf. infra, ch. 3.1, commentaire relatif à l'art. 26 LCPD). Cela ne figure toutefois pas dans la loi sur la protection des données. En ce qui concerne la procédure et la protection juridique, l'article 26 LCPD renvoie uniquement aux dispositions de la loi sur la procédure et la juridiction administratives et de la loi sur les communes, ce qui, dans la pratique, a soulevé des questions liées aux voies de recours. Une version plus précise de l'article 26 LCPD doit permettre de lever ces incertitudes.

2.3 Statut de l'autorité de surveillance de la protection des données

2.3.1 Principe de l'indépendance

Selon l'article 28, alinéa 1 de la directive de l'UE, les autorités chargées de surveiller l'application des dispositions en matière de protection des données «exercent en toute indépendance les missions dont elles sont investies». Le Protocole additionnel exige lui aussi que les autorités de contrôle exercent leurs fonctions «en toute indépendance» (préambule et art. 1, ch. 3). Un tel principe doit être consigné expressément dans la loi.

L'indépendance de l'autorité de surveillance de la protection des données présuppose des «garanties» organisationnelles adaptées. Il convient d'assurer, par une réglementation adéquate portant sur la désignation et sur le statut juridique des personnes responsables ainsi que par la position au sein de l'administration de l'autorité de surveillance que les personnes qui en font partie disposent de suffisamment d'indépendance envers l'administration qu'elles contrôlent pour qu'elles ne soient par exemple pas entravées dans l'exercice de leurs fonctions par la menace d'un licenciement. Différentes solutions permettent d'appliquer concrètement une telle prescription. Il est essentiel que les réglementations garantissent intégralement que l'autorité de surveillance de la protection des données puisse travailler «en toute indépendance», comme cela est exigé. A cet égard, il convient de prendre en compte les modalités de l'organisation de l'autorité de surveillance.

2.3.2 Organisation de l'autorité de surveillance cantonale

Contrairement à la proposition émise par le Conseil-exécutif dans le projet de loi cantonale sur la protection des données de 1985, qui prévoyait d'octroyer à l'autorité de surveillance un statut de commission, le Grand Conseil décida alors, suivant en cela la proposition de la commission consultative, de charger de la surveillance un délégué à la protection des données. Cette solution a fait ses preuves dans la pratique. Selon le Conseil-exécutif, il n'existe aucune raison de revenir sur cette décision prise autrefois par le Grand Conseil. Au vu des prescriptions européennes, les arguments en faveur d'une commission qu'il avait avancés en son temps n'ont plus guère de poids. En raison des nouvelles tâches contraignantes qu'il s'agira d'assumer dans le domaine de la surveillance de la protection des données (cf. ch. 2.4 infra), une «commission de milice», économiquement avantageuse, ne pourrait plus entrer en ligne de compte. Le système actuel permet, en fonction des besoins, de chercher à l'extérieur des informations spécifiques, pour autant que la personne déléguée à la protection des données n'en dispose pas elle-même. Enfin, un autre argument s'opposant à la création d'une commission est la lourdeur que représente une telle solution. En effet, une commission réagit plus lentement qu'une personne seule, ce qui aurait des répercussions négatives avant tout sur l'exécution des affaires courantes.

Il n'y a aucune raison non plus de donner à l'autorité de surveillance la forme d'une unité administrative. La «personnification» liée à un délégué ou à une déléguée à la protection des données apparaît plus favorable, d'un point de vue psychologique tout au moins, parce que les intéressés peuvent s'identifier à une telle personne et qu'ils s'y adressent plus volontiers qu'à une unité administrative «anonyme». Du point de vue du volume limité en termes d'activité et de ressources, la constitution d'une telle unité à part entière paraît également disproportionnée. Sur ce point-là, l'autorité de surveillance de la protection des données ne peut être comparée par exemple au Contrôle des finances cantonal.

Par conséquent, il convient de maintenir la solution actuelle d'une personne déléguée à la protection des données qui correspond au système largement répandu tant à l'étranger qu'en Suisse, et notamment à ce qui prévaut au niveau fédéral (art. 26 ss LPD). Il n'est pas exclu que dans le cadre des ressources accordées au niveau budgétaire, d'autres personnes disposant de connaissances spécifiques (en droit, en informatique) puissent, selon les circonstances, traiter de questions en relation avec la protection des données sous la responsabilité du délégué ou de la déléguée.

2.3.3 Garanties d'indépendance institutionnelles

a) Election ou désignation de la personne déléguée au niveau cantonal

A l'heure actuelle, le Conseil-exécutif désigne l'autorité cantonale de surveillance en la personne d'un délégué à la protection des données (art. 32, al. 1 LCPD). Par rapport aux prescriptions européennes, cette réglementation paraît certes possible, mais ne va pas sans poser quelques problèmes, puisque selon le guide de la CdC, «une élection par l'exécutif uniquement constitue une élection des contrôleurs par

les contrôlés» et qu'elle peut «sous l'angle de l'indépendance totale exigée, tout au plus suffire si ce déficit évident est compensé par d'autres garanties de qualité plus élevée», en particulier une durée de fonction relativement longue (un mandat de huit ans ou plus selon le guide). Lors de la création de la loi sur la protection des données, la Direction de la justice d'alors avait déjà proposé une élection formelle par le Grand Conseil de la personne déléguée à la protection des données, dans une volonté de respect de l'indépendance. Au vu surtout des nouvelles prescriptions européennes, plusieurs arguments, dont les suivants, parlent en faveur d'une telle solution:

– L'indépendance de l'autorité de surveillance de la protection des données envers le gouvernement et l'administration est garantie dès sa désignation. Il est ainsi tenu compte de manière optimale des prescriptions du droit européen: avec une telle solution, le canton fait le choix de la sécurité.
– Il est possible d'éviter toute insécurité juridique. Si la personne continuait à être désignée par le Conseil-exécutif, comme c'est le cas actuellement, la réglementation devrait être complétée par «d'autres garanties de niveau de qualité très élevé» dont le contenu détaillé n'apparaît pas clairement.
– Il semble politiquement souhaitable que l'on évite ne serait-ce que l'apparence d'une dépendance à l'égard de l'organe exécutif et de l'administration, ce qu'offre une élection par le Grand Conseil.

A l'inverse, le maintien de la désignation par le Conseil-exécutif pourrait cependant se justifier par le fait que cet organe, grâce à sa connaissance de l'administration, est mieux à même de juger les aptitudes professionnelles des personnes entrant en ligne de compte. Il est toutefois possible de tenir compte de cela si le Grand Conseil élit la personne sur proposition du Conseil-exécutif. Pour les raisons d'ordre juridique et politique évoquées, une élection formelle par le Grand Conseil paraît donc indiquée. Une telle élection ne devrait pas impliquer un travail supplémentaire important pour le Grand Conseil puisqu'elle n'aura en principe lieu qu'au début de chaque période de fonction (voir le ch. 2.3.3 b infra).

b) Période de fonction

La loi sur la protection des données ne contient aucune disposition particulière sur le statut juridique de la personne déléguée à la protection des données, celle-ci étant soumise à un rapport de service de droit public résiliable d'une durée indéterminée au sens des articles 37 et suivants de la loi du 16 septembre 2004 sur le personnel (LPers)[15]. Afin de garantir l'indépendance totale exigée, la personne déléguée à la protection des données devra être élue à l'avenir pour une période de fonction fixe. Dans le canton de Berne, la durée des mandats est habituellement de quatre ans. Dans des cas particuliers, notamment pour les ecclésiastiques[16] ainsi que pour les membres de la Cour suprême[17] et du Tribunal administratif[18], la période de fonction est de six ans. Le fait de proposer une élection par le Grand Conseil offre une légitimité démocratique élevée, raison pour laquelle la période de fonction de quatre ans, qui est usuelle dans le canton, paraît ici appropriée.

Une limitation du nombre de réélections peut certes prévenir le risque que la personne déléguée à la protection des données devienne, au fil du temps, trop proche des autorités qu'elle est chargée de contrôler. Toutefois, il ne faut pas oublier non plus que ce domaine-là exige des compétences professionnelles particulières ainsi qu'une certaine expérience. L'idée d'une restriction légale de la durée du mandat est ainsi rejetée, ce qui implique qu'en principe, la personne déléguée à la protection des données peut être réélue de manière illimitée.

c) Ressources

L'indépendance de l'autorité de surveillance de la protection des données ne peut être garantie qu'à la condition que l'administration qui doit subir les contrôles ne puisse pas entraver ou influencer la planification et la mise en œuvre de l'activité de surveillance en privant l'autorité des ressources nécessaires. Or, dans la pratique, des problèmes à ce niveau-là ont clairement été constatés. La Commission de gestion du Grand Conseil, relevait, au sujet du rapport de gestion 2000, «l'impossibilité chronique dans laquelle [le délégué] est de remplir comme il se doit le mandat légal de la protection des données» et recommandait au gouvernement de mettre à disposition les ressources humaines nécessaires à cet égard. Le Conseil-exécutif a repris une telle recommandation dans trois arrêtés visant à décharger le Bureau pour la surveillance de la protection des données (mise en place d'organes de contrôle externes; décision de faire des services juridiques les interlocuteurs en matière de protection des données au sein de l'administration; obligation d'établir des schémas de protection des données concernant les projets informatiques). Il a aussi pris connaissance du fait que le Bureau avait classé sans les traiter 120 dossiers en suspens. Ce n'est donc pas sans raison que les prescriptions européennes exigent expressément des garanties légales. Elles prévoient que l'autorité de surveillance doit disposer de son propre budget pour les ressources humaines et matérielles dont elle a besoin, qui est adopté par l'organe compétent, c'est-à-dire le Grand Conseil, «sans intervention du gouvernement». La personne ou le service responsable de la surveillance de la protection des données doit également avoir la possibilité d'engager directement, dans le cadre du budget, le personnel dont elle ou il a besoin pour assumer ses fonctions. Cela correspond à la réglementation en vigueur par exemple pour le Contrôle des finances ou pour les instances judiciaires. Il faut également que l'autorité de surveillance puisse disposer de liberté s'agissant de l'utilisation des ressources et avoir par exemple la possibilité de s'adresser à des spécialistes extérieurs en cas de surcharge.

[15] RSB 153.01
[16] Art. 32, al. 1 de la loi du 6 mai 1945 sur les Eglises nationales bernoises (RSB 410.1)
[17] Art. 4, al. 1 de la loi du 14 mars 1995 sur l'organisation des juridictions civile et pénale (LOJ; RSB 161.1)
[18] Art. 120, al. 1 LPJA, teneur du 14 mars 1995

d) Rattachement administratif

A l'heure actuelle, l'autorité cantonale de surveillance en matière de protection des données est administrativement rattachée à la Direction de la justice, des affaires communales et des affaires ecclésiastiques (art. 32, al. 2 LCPD). A ses débuts, cette autorité avait été comprise avant tout comme un «service spécial» s'occupant principalement de questions d'ordre juridique. Une véritable intégration de l'autorité de surveillance à l'administration, conçue comme une subordination hiérarchique à une Direction avait été exclue lors de l'édiction de la loi sur la protection des données déjà, car l'indépendance de cette autorité aurait ainsi été remise en cause. Une telle situation ne répond pas en particulier aux exigences posées par les accords de Schengen/Dublin, qui prévoient que l'autorité de surveillance doit agir «en toute indépendance». En revanche, il est possible de prévoir, tout en respectant le droit européen, un rattachement purement administratif de l'autorité de surveillance à une Direction, tout comme il est envisageable de l'associer au Bureau du Grand Conseil ou à la Chancellerie d'Etat.

Le guide de la CdC recommande d'attribuer l'autorité de surveillance pour la protection des données, en cas d'élection par le parlement, au «bureau du Parlement», soit, dans le cas d'espèce, au Bureau du Grand Conseil. Le Conseil-exécutif estime cependant qu'un tel rattachement est inadéquat car s'il est vrai que la personne déléguée à la protection des données doit être indépendante du Conseil-exécutif et de l'administration, elle n'assume aucune fonction parlementaire, mais bel et bien une fonction administrative. L'indépendance est suffisamment garantie grâce à l'élection par le Grand Conseil qui est proposée et la période de fonction fixe. L'autorité de surveillance ne doit par ailleurs entretenir aucun contact régulier avec le Grand Conseil, mais lui adresser simplement un rapport périodique sur ses activités (cf. art. 37, al. 1 LCPD), comme le font le Conseil-exécutif et, par exemple, le Contrôle des finances. Un rattachement de l'autorité de surveillance au Bureau du Grand Conseil apparaît donc inadapté.

Le rattachement à une Direction peut quant à lui, théoriquement et d'un point de vue extérieur, laisser penser qu'il existe une certaine dépendance de l'autorité de surveillance à l'égard des instances dirigeantes de la Direction et donc éveiller des soupçons de prévention. On ne saurait toutefois accorder trop de poids à un tel argument, notamment au vu des «garanties» d'indépendance qui ont par ailleurs été prévues (cf. ch. 2.3.3 a à c supra). A cet égard, le rattachement de l'autorité de surveillance à la JCE n'a jusqu'à maintenant pas posé de problème majeur s'agissant de son indépendance. Pour des raisons pragmatiques, le projet d'adaptation de la loi sur la protection des données prévoit donc que le Bureau cantonal pour la surveillance de la protection des données continuera d'être administrativement rattaché à la Direction de la justice, des affaires communales et des affaires ecclésiastiques.

2.3.4 Surveillance de la protection des données relative aux prestataires de soins au sens de la loi sur les soins hospitaliers

S'agissant de l'organisation de la surveillance de la protection des données, un problème particulier concerne la surveillance des prestataires au sens de la loi du 5 juin 2005 sur les soins hospitaliers (LSH)[19]. Selon l'article 77 LSH, le Conseil-exécutif peut prévoir par voie d'ordonnance que les prestataires de soins remplissant des tâches cantonales doivent désigner une autorité de surveillance pour la protection des données. En pareil cas, le Bureau de surveillance cantonal au sens de l'article 32 LCPD exerce la haute surveillance. Les syndicats hospitaliers étaient jusqu'à maintenant tenus, en leur qualité de collectivités de droit communal, de disposer de leur propre autorité de surveillance de la protection des données. L'article 77 LSH devait assurer que les ressources à cet égard seraient toujours disponibles, même après la cantonalisation des hôpitaux publics.

Le Conseil-exécutif a fait usage de sa compétence et a obligé, par l'article 110 de l'ordonnance du 30 novembre 2005 sur les soins hospitaliers (OSH)[20] les prestataires de soins hospitaliers et préhospitaliers qui remplissent des tâches cantonales sans faire partie de l'administration cantonale à désigner une autorité de surveillance commune indépendante pour la protection des données. Cette autorité n'existe pas encore. On peut maintenant se demander, à la lumière des prescriptions prévues par les accords de Schengen/Dublin, si une telle disposition doit être maintenue. La complexité du domaine due notamment aux systèmes d'informations cliniques (gestion électronique des dossiers des patients) et les exigences élevées de professionnalisme posées aux personnes responsables parlent en faveur d'une autorité centrale de surveillance dans le secteur hospitalier également. Une centralisation permettrait en effet de simplifier le processus puisqu'il y aurait une surveillance unique des trois cliniques psychiatriques cantonales faisant partie de l'administration cantonale ainsi que des autres hôpitaux et que la haute surveillance exercée par la personne déléguée à la protection des données n'aurait plus de raison d'être. Une telle solution suivrait en définitive l'approche de cantonalisation des hôpitaux voulue par la loi sur les soins hospitaliers. Pour ces différentes raisons, le Conseil-exécutif considère la possibilité de réviser ou d'abroger l'article 110 OSH en vue de transmettre la surveillance des hôpitaux en matière de protection des données au délégué cantonal. Il s'agit encore d'examiner de plus près la façon dont les prestataires au sens de la loi sur les soins hospitaliers peuvent financer cette activité.

Une éventuelle modification de l'ordonnance sur les soins hospitaliers n'a toutefois aucun impact sur l'activité législative qui est du ressort du Grand Conseil. L'article 77 LSH ne contient en effet qu'une simple prescription potestative qui habilite le Conseil-exécutif à arrêter des dispositions. Cette prescription peut être conservée même si le délégué cantonal à la protection des données assume la surveillance sur les hôpitaux.

[19] RSB 812.11
[20] RSB 812.112

2.3.5 Surveillance de la protection des données dans les communes

Pour les communes et les autres collectivités de droit communal, la loi sur la protection des données s'applique de manière générale de la même façon que pour le canton. Les dispositions sur l'indépendance de l'autorité de surveillance ainsi que les compétences et tout particulièrement les tâches et les pouvoirs de l'autorité décrits plus précisément sous le chiffre 2.4 infra concernent également les collectivités de droit communal. Les exigences à l'égard des autorités de surveillance communales en matière d'organisation et de compétences professionnelles sont donc élevées et représentent d'ailleurs un excellent argument en faveur d'une cantonalisation de la surveillance de la protection des données dans les communes. Ce sont surtout les collectivités de droit communal de petite taille qui doivent éprouver de la difficulté à créer un organe de surveillance doté des compétences nécessaires.

Dans le cadre de la présente révision, conformément aux idées directrices mentionnées (cf. ch. 1.4 supra), seules sont proposées des adaptations plus ou moins imposées par les prescriptions européennes ou par d'autres motifs. Il n'existe aucun besoin impérieux justifiant une modification allant dans le sens d'une cantonalisation de la surveillance de la protection des données dans les communes car le droit européen ne prescrit rien de tel. Le statut des autorités communales de surveillance est en principe compatible avec les accords de Schengen/Dublin. Si l'on tient compte de la garantie de l'autonomie communale prévue par la Constitution et de l'obligation faite au canton d'accorder aux communes «la plus grande liberté de décision possible» (art. 109, al. 2 ConstC), il paraît correct de maintenir le système actuel des autorités de surveillance de la protection des données propres aux communes, notamment parce que dans le domaine de la police, qui est une composante centrale des accords de Schengen/Dublin, les communes, en raison de l'application du projet «Police Bern», ne pourront plus disposer que de compétences limitées. Elles n'auront plus guère à s'occuper du traitement de données réellement importantes au sens de ces accords. Il convient aussi de tenir compte du fait que l'autorité de surveillance cantonale exerce la haute surveillance sur les services communaux (art. 33, al. 2 LCPD).

La loi sur la protection des données doit respecter les dispositions européennes, et en particulier le Protocole additionnel, en prescrivant de manière générale que les autorités communales de surveillance assument elles aussi leurs fonctions en toute indépendance et que les communes prévoient à cet égard des garanties de type organisationnel ou institutionnel. Il revient aux communes, dans le cadre de l'autonomie dont elles disposent en matière d'organisation, de décider de la manière dont elles appliquent ces prescriptions contraignantes. Elles doivent cependant être soutenues en recevant des informations adéquates – qui peuvent prendre la forme de documents ISCB ou d'un règlement type actualisé sur la protection des données – sur les exigences juridiques auxquelles doit répondre l'autorité de surveillance de la protection des données et en particulier sur son indépendance et ses possibilités d'intervention. Les collectivités de droit communal qui ne répondent pas aux exigences du droit européen devront être invitées à apporter les améliorations nécessaires. Au vu de ce qui est présenté sous le chiffre 2.3.3, les solutions prévoyant que l'autorité de surveillance est intégrée à un service juridique communal ou qu'elle remplit un mandat à l'égard de la commune, que l'organe exécutif de cette dernière peut résilier à tout moment, peuvent être considérées comme délicates d'un point de vue juridique.

2.4. Tâches et compétences des autorités de surveillance

2.4.1 Traitement des requêtes

L'article 28, alinéa 4 de la directive de l'UE prévoit que «chaque autorité de contrôle peut être saisie par toute personne [...]», personne concernée étant «informée des suites données à sa demande». La requête devra faire l'objet d'un examen lorsque le droit à obtenir des renseignements dans les domaines de la police, de la poursuite pénale et de la protection de l'Etat est limité en raison de prescriptions particulières. La loi cantonale sur la protection des données en vigueur ne prévoit aucune obligation de traiter des requêtes portant sur le traitement de données personnelles mais renvoie, à l'article 26 LCPD, à la loi sur la procédure et la juridiction administratives en ce qui concerne la procédure d'ordre général. Selon l'article 101 LPJA, la personne qui dénonce à l'autorité de surveillance peut demander que des informations sur la liquidation de sa dénonciation lui soient fournies. Il n'existe pas de droit au traitement matériel et à la liquidation de la requête. Une telle réglementation ne satisfait pas entièrement aux dispositions du droit européen mentionnées, car elle ne prévoit d'obligation de renseigner sur le traitement des requêtes relevant du droit de la surveillance que sur demande. Il convient de donner une portée générale à une telle obligation dans la mesure où le droit de consulter ses propres données est limité dans les domaines de la police, de la poursuite pénale et de la protection de l'Etat.

2.4.2 Pouvoirs d'investigation, contrôles préalables

L'article 28, alinéa 3 de la directive de l'UE prévoit que l'autorité de surveillance dispose de «pouvoirs d'investigation». Selon l'article 35, alinéa 2 LCPD, l'autorité de surveillance peut, en dépit d'éventuelles obligations de garder le secret, recueillir des informations écrites ou orales auprès des autorités. Elle a accès à tous les documents utilisés pour des traitements déterminés, peut effectuer des visites et se faire présenter le traitement de données. Les autorités responsables sont tenues d'assister l'autorité de surveillance dans l'accomplissement de ses tâches (art. 35, al. 1 LCPD). Par cette disposition, des pouvoirs d'investigation complets sont octroyés à l'autorité de surveillance et, de ce point de vue-là, les exigences européennes sont suffisamment respectées.

Il n'en va pas de même pour le cas précis de ce que l'on nomme les contrôles préalables, un domaine qu'il convient donc de réglementer. L'article 20, alinéa 1 de la directive de l'UE oblige les Etats membres à préciser les traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées et à veiller à ce que ces traitements soient examinés avant leur mise en œuvre. L'alinéa 2 du même article prévoit que «de tels examens préalables sont

effectués par l'autorité de contrôle après réception de la notification du responsable du traitement ou par le détaché à la protection des données, qui, en cas de doute, doit consulter l'autorité de contrôle». Jusqu'à maintenant, de tels contrôles préalables n'ont fait l'objet d'aucune réglementation légale dans le canton de Berne. Aucune prescription ne s'applique aux collectivités de droit communal. En ce qui concerne l'administration cantonale, un arrêté du Conseil-exécutif du 9 avril 2003 prévoit que lorsqu'un projet informatique entraîne des coûts supérieurs à 100 000 francs, ses responsables doivent élaborer un schéma de protection des données qui doit être soumis à l'autorité de surveillance pour examen avant que l'arrêté de dépense ne soit rendu. Il en va de même lorsque le canton verse à des tiers, par exemple à des hôpitaux, des contributions à des projets informatiques. L'article 52, alinéa 5 de la loi du 8 juin 1997 sur la police (LPol)[21)] prévoit un instrument analogue à un examen préalable puisqu'il exige une autorisation d'exploitation du Conseil-exécutif pour les systèmes informatiques de la Police cantonale. Dans la pratique, une prise de position a été demandée pour chaque cas à l'autorité de surveillance de la protection des données, bien qu'elle ne soit pas prescrite par la loi.

Le Conseil-exécutif envisage, indépendamment des accords de Schengen/Dublin, une procédure différenciée lors de l'introduction de nouveaux projets informatiques du canton qui accorderait tout le poids nécessaire à l'examen préalable du point de vue du droit de la protection des données. Pour l'administration cantonale et les contributions cantonales, un tel procédé s'avère suffisant pour satisfaire aux prescriptions du droit européen, mais il doit être ancré dans une loi. Il convient en outre de légiférer sur les contrôles préalables pour les systèmes informatiques des collectivités de droit communal.

2.4.3 Pouvoirs d'intervention

L'article 28, alinéa 3 de la directive de l'UE exige des «pouvoirs effectifs d'intervention» de l'autorité de surveillance et énumère ce qu'il faut comprendre par là. Il peut s'agir par exemple de la compétence d'assurer une publication appropriée des avis, d'ordonner le verrouillage, l'effacement ou la destruction de données ou d'interdire définitivement un traitement de données, d'adresser un avertissement ou une admonestation au responsable du traitement ou de saisir les parlements nationaux ou d'autres institutions politiques. Aucun «degré minimal» précis de pouvoirs effectifs n'est expressément prescrit. Il est cependant nécessaire que l'autorité de surveillance puisse véritablement faire preuve d'efficacité en déployant dans leur intégralité les pouvoirs d'intervention établis légalement. Par conséquent, il faut en cas d'urgence qu'elle soit en mesure d'appliquer les prescriptions légales liées à la protection des données, même en s'opposant à une autorité.

L'actuelle réglementation ne répond pas à cette exigence. Pour l'instant, l'autorité de surveillance a en principe uniquement la possibilité de recommander de remédier à des irrégularités et de combler des lacunes ainsi que de présenter des propositions d'amélioration de la protection des données (art. 35, al. 3 LCPD; au sujet de la compétence décisionnelle prévue par l'article 27 – qui, dans la pratique, ne déploie pratiquement aucun effet – cf. infra ch. 3.1, commentaire relatif à l'art. 27). Si le service responsable du traitement des données ne suit pas une recommandation, l'autorité de surveillance ne dispose d'aucune possibilité de prendre des mesures contraignantes et d'imposer son avis contre la volonté du service concerné. Elle peut uniquement demander à l'autorité responsable ou à son autorité supérieure de prendre les mesures qui s'imposent (art. 35, al. 4 LCPD) et informer le public (art. 37, al. 2 LCPD), en exerçant ainsi une forme de pression.

Il est possible de tenir compte de différentes manières de cette prescription sur les pouvoirs effectifs d'intervention. Les options suivantes se présentent notamment:

Variante a)

L'autorité de surveillance décide seule lorsque cela s'avère nécessaire. Elle émet ses recommandations à l'autorité concernée sous la forme d'une instruction contraignante qui a le même effet qu'une décision envers des tiers au sens de l'article 49 LPJA.

Variante b)

L'autorité de surveillance jouit en principe des compétences que lui confère le droit en vigueur. En raison des droits complets dont elle dispose en matière de renseignement et d'examen, elle peut transmettre des recommandations aux autorités chargées du traitement des données sur la façon de concevoir ou d'effectuer le traitement des données conformément au droit et à la protection des données. Dans ce contexte, elle ne peut en principe émettre elle-même aucune instruction à caractère obligatoire, mais exiger, pour le cas où la recommandation ne serait pas suivie, que l'autorité traitant les données notifie le refus complet ou partiel des recommandations au moyen d'une décision au sens de l'article 49 LPJA ou d'une autre décision à caractère contraignant dans les procédures auxquelles s'applique le Code de procédure civile ou le Code de procédure pénale. La décision peut être attaquée par l'autorité de surveillance au moyen d'un recours des autorités auprès des instances juridictionnelles compétentes. L'autorité de surveillance a ainsi la possibilité d'obtenir un jugement contraignant sur la légalité du traitement des données contesté.

Variante c)

Une autre option partiellement comparable à la variante b) se fonde sur le droit fédéral, à savoir sur l'article 27, alinéas 4 à 6 LPD. Comme dans le cas de la variante b), l'autorité de surveillance émet une recommandation et en informe le département compétent ou la Chancellerie fédérale. Si une recommandation est rejetée ou n'est pas suivie, l'autorité de surveillance peut porter l'affaire pour décision devant le département ou la Chancellerie fédérale, mais aussi recourir ensuite si nécessaire contre la décision de ces autorités.

Le fait qu'avant même l'émission d'une instruction à caractère obligatoire, trois services soient impliqués dans la procédure prévue par la variante c) présente un inconvénient. Celle-ci est donc relativement compliquée et pourrait entraîner des

[21)] RSB 551.1

retards, tout en n'apportant aucun avantage notable par rapport à la variante b). Le Conseil-exécutif n'entre donc pas en matière sur cette variante c). En revanche, plusieurs arguments parlent en faveur des deux autres variantes. Pour le Conseil-exécutif, les avantages de la variante b) sont nettement prédominants et il lui accorde sa préférence pour les raisons suivantes:

- La variante b) décharge l'autorité de surveillance de la protection des données et ménage ses ressources. Le travail qu'implique une recommandation sera nettement moins important que le prononcé d'une décision formelle. Du point de vue du contenu, des instructions à caractère obligatoire devraient faire l'objet d'une vérification plus approfondie et impliqueraient également, du point de vue du droit procédural, des tâches supplémentaires (p. ex. droit d'être entendu). Si l'autorité concernée suit la recommandation, l'affaire est liquidée.
- La variante b) correspond au principe selon lequel la responsabilité d'un traitement des données conforme à la loi incombe à l'autorité qui traite les données (art. 8, al. 1 LCPD). Une telle responsabilité n'aurait plus la même portée si l'autorité de surveillance pouvait émettre des instructions contraignantes.
- La variante b) fait dans une certaine mesure appel au principe de causalité. L'autorité qui traite les données décide elle-même de la façon dont elle assume ses tâches, mais elle doit tenir compte du fait que, le cas échéant, le non-respect d'une recommandation de l'autorité de surveillance peut nécessiter un travail supplémentaire. En effet, elle devra confirmer sa vision juridique sous la forme d'une décision, la motiver de manière détaillée et, si nécessaire, la défendre dans une procédure de recours. Les frais dus au règlement des différends sont ainsi mis à la charge de la partie qui prétend disposer de motifs suffisants pour ne pas suivre une recommandation.
- La prescription directe et obligatoire de mesures au sens de la variante a) contredirait la vision suisse d'une autorité de surveillance de la protection des données qui doit avant tout prodiguer des conseils et offrir un soutien.
- Dans le cas de la variante b), il existe toujours la possibilité que le service traitant les données et l'autorité de surveillance de la protection des données cherchent en premier lieu le dialogue et trouvent une solution à l'amiable. Le statut d'organe indépendant offrant des conseils dont jouit l'autorité de surveillance s'en trouve ainsi tout particulièrement renforcé.
- Enfin, la variante b) présente également des avantages du point de vue du droit procédural. Les voies de recours existantes, prévues par les dispositions de droit procédural en vigueur de la loi sur la procédure et la juridiction administratives, du Code de procédure civile et du Code de procédure pénale ou, le cas échéant, de la législation spéciale, peuvent s'appliquer sans modification. L'autorité de surveillance peut attaquer la décision en question au même titre qu'un particulier dans le cadre de la procédure légale prévue aujourd'hui déjà.

Au vu des motifs exposés, il apparaît approprié de s'en tenir, comme le prévoit la variante b), à l'instrument de la recommandation, en l'associant cependant à la possibilité offerte au Bureau pour la surveillance de la protection des données d'amener l'autorité à rendre une décision négative. Ce procédé permet également, au besoin, d'obtenir un jugement contraignant d'un tribunal sur la base des prescriptions de droit procédural applicables (LPJA, le cas échéant, CPC ou CPP). De l'avis du Conseil-exécutif, les arguments en faveur de la variante a) n'ont pas un poids suffisant par rapport à la variante b). Le fait que cette dernière prévoie, le cas échéant, une procédure de recours interne à l'administration avant l'examen par un tribunal en cas d'application de la loi sur la procédure et la juridiction administratives ne constitue pas un inconvénient majeur. Le risque que l'autorité responsable renonce au prononcé d'une décision négative et accepte apparemment la recommandation mais ne mette pas l'instruction en œuvre par la suite ne peut certes pas être exclu mais, si l'on en croit les expériences réalisées à ce jour, reste largement théorique. En cas de carence de l'autorité, qui refuserait de statuer ou tarderait à se prononcer, il serait possible, si nécessaire, de recourir (cf. en particulier l'art. 49, al. 2 LPJA).

2.4.4 Pouvoir d'ester en justice et d'avertir l'autorité, sanctions

L'article 28, alinéa 3 de la directive de l'UE prévoit le «pouvoir d'ester en justice» en cas de violation des dispositions prises en application de la directive ou le «pouvoir de porter ces violations à la connaissance» de l'autorité de surveillance de la protection des données. Ce qui est nécessaire en l'occurrence n'est pas un véritable droit d'intenter une action, mais un droit de dénoncer en cas de violation de la loi sur la protection des données et d'obtenir l'application d'une sanction pénale. Il suffit par conséquent que l'autorité de surveillance ait la possibilité de dénoncer un cas à l'autorité de poursuite pénale. Cette exigence est remplie. Si l'autorité de surveillance de la protection des données a connaissance d'un acte punissable se poursuivant d'office, elle a le droit ou même l'obligation, en vertu des articles 199 et 201 CPP, de le dénoncer à la police ou à une autre autorité de poursuite pénale. Lors de violations constatées ou présumées de la loi sur la protection des données, elle a en outre toujours la possibilité d'émettre des recommandations (art. 35, al. 3 LCPD), indépendamment du caractère punissable de l'action en question, ou de dénoncer le cas à l'autorité de surveillance (art. 101 LPJA).

Selon l'article 24 de la directive de l'UE, les violations des dispositions de la législation sur la protection des données donnent lieu à des sanctions. L'article 320 du Code pénal suisse du 21 décembre 1937 (CPS)[22)] offre une protection de droit pénal contre les violations du secret de fonction par les autorités traitant les données. Les tiers qui traitent des données personnelles sur mandat d'une autorité sont également soumis au secret de fonction (art. 16 LCPD). Si des tiers mandatés communiquent des données en violation de leur mandat, on peut considérer que l'on est en présence d'une violation du secret de fonction, raison pour laquelle, dans un tel cas, la réglementation actuelle du Code pénal suisse s'avère suffisante. Cependant, des violations de la loi sur la protection des données commises par les autorités traitant les données elles-mêmes ou par des tiers mandatés qui ne tombent pas sous le coup de la violation du secret de fonction sont également imaginables. Ainsi, selon l'article 5, alinéa 4 LCPD, il est interdit de traiter des données personnelles dans un but qui, en vertu du principe de la bonne foi, est incompatible avec le but en vue

[22)] RSB 311.0

duquel elles avaient été recueillies ou communiquées à l'autorité. A l'heure actuelle, dans de tels cas, seul le caractère illicite de l'acte peut être constaté, mais aucune sanction pénale ne peut être prononcée. Bien qu'une telle possibilité paraisse souhaitable, il s'agirait de résoudre en premier lieu ce problème dans le cadre d'une réglementation de droit fédéral à intégrer au Code pénal suisse. L'édiction d'une disposition spéciale de droit pénal cantonal semble donc inopportune.

2.4.5 Entraide administrative

L'article 28, alinéa 6 de la directive de l'UE et l'article 1, chiffre 5 du Protocole additionnel obligent les autorités de surveillance de la protection des données à coopérer pour accomplir leurs tâches de contrôle et à s'accorder mutuellement une entraide administrative. Il s'agit ici de coopérer aussi bien avec les autorités de surveillance d'autres cantons et de la Confédération qu'avec les services concernés à l'étranger. Etant donné que le canton de Berne dispose également d'organes de surveillance communaux, il convient aussi de réglementer l'obligation de coopérer à l'intérieur du canton. Certes, le droit en vigueur contient déjà des dispositions sur la coopération. Ainsi, la disposition potestative de l'article 36a, alinéa 1 LCPD autorise l'autorité cantonale de surveillance à coopérer en vue d'accomplir ses tâches avec les organes de surveillance de la protection des données d'autres collectivités de droit public, le type et l'étendue de la coopération étant définis dans une convention écrite (art. 36a, al. 2 LCPD). Cette réglementation a été intégrée à la loi sur la protection des données lors de l'adoption de la loi du 5 juin 2002 sur la société anonyme Bedag Informatique (loi sur la Bedag, LBI)[23] et devait, par la participation du canton de Vaud à la Bedag, permettre des inspections communes des autorités cantonales de surveillance des cantons de Berne et de Vaud. Mais l'entraide administrative à proprement parler, au sens de l'article 28, alinéa 6 de la directive de l'UE n'est pas traitée par cette disposition. De même, les dispositions de portée générale sur la coopération entre la Confédération et les cantons prévues à l'article 44 Cst. et sur le concours réciproque que se doivent les autorités administratives et de justice administrative selon l'article 10 LPJA semblent insuffisantes, en particulier en ce qui concerne la coopération avec des autorités de surveillance étrangères.

2.4.6 Autres points

La présente révision partielle permet enfin de supprimer la disposition sur la compétence décisionnelle de l'autorité de surveillance, qui n'a aucune signification pratique et de réglementer également sous une nouvelle forme son obligation de rendre compte de ses activités (cf. infra ch. 3.1, commentaires relatifs aux art. 27 et 37 LCPD).

[23] RSB 152.031.2

3. Commentaires des différentes dispositions

3.1 Loi sur la protection des données

Article 4: Champ d'application

Conformément à la disposition du droit fédéral (art. 2, al. 2, lit. *c* LPD), le champ d'application de la loi sur la protection des données est étendu, par l'article 4, alinéa 2, lettre *c* LCPD, à la procédure administrative, c'est-à-dire à la procédure préalable au prononcé d'une décision (art. 49 à 59 LPJA) (cf. aussi ch. 2.2.1 supra). Pour les procédures de justice administrative, procédure de recours interne à l'administration incluse, seules les dispositions de la loi sur la procédure et la juridiction administratives sont applicables. La modification implique une adaptation de l'article 23 LPJA (cf. ch. 3.2 infra).

Article 14a (nouveau): Communication de données à l'étranger

Le nouvel article 14a permet d'intégrer à la loi la réglementation nécessaire sur la communication de données à l'étranger. La disposition s'inspire largement de la réglementation fédérale prévue à l'article 6 de la version révisée de la loi sur la protection des données, par lequel la Confédération adapte sa législation aux prescriptions prévues par le Protocole additionnel.

L'alinéa 1 reprend de manière littérale l'article 6, alinéa 1 LPD révisée. L'alinéa 2 prévoit diverses conditions permettant de s'écarter du principe de l'alinéa 1. Comme le montre le mot «ou» placé à la fin de la lettre *e*, il s'agit de possibilités non cumulatives. Pour que la communication des données soit admissible, il suffit par conséquent que l'une des conditions citées soit remplie. L'énumération est par ailleurs exhaustive, ce qui signifie qu'il faut être en présence de l'une au moins des situations prévues à l'alinéa 2 pour qu'il y ait menace au sens de l'alinéa 1. D'éventuelles prescriptions de lois spéciales qui autorisent une communication dans d'autres cas sont réservées. Si l'on excepte le mot «ou» placé à la fin de la lettre *e*, l'alinéa 2 correspond mot à mot à la réglementation de l'article 6, alinéa 2 LPD révisée, la lettre *f* de cette disposition n'ayant cependant pas été reprise. L'article 6, alinéa 2, lettre *f* de la loi sur la protection des données révisée autorise la communication de données même si la personne concernée les a rendues accessibles à tout un chacun en ne s'opposant pas formellement à leur traitement. A une telle condition, la communication de données selon le droit fédéral est également autorisée en Suisse (art. 17, al. 2, lit. *c* LPD). La loi cantonale sur la protection des données réglemente de manière plus restrictive, aux articles 10 et 11, la communication de données en Suisse. Si l'article 6, alinéa 2, lettre *f* LPD était introduit dans la loi cantonale, ce type de données pourraient être communiquées aisément à l'étranger mais ne le seraient en Suisse que dans le cadre restreint des articles 10 et 11, alinéa 2 LCPD. Les destinataires en Suisse seraient ainsi moins bien placés que ceux de l'étranger. Il est possible d'éviter une conséquence aussi choquante en ne reprenant pas dans la loi cantonale sur la protection des données l'article 6, alinéa 2, lettre *f* LPD qui convient certes au droit fédéral, mais non au droit cantonal.

Dans l'intérêt des personnes concernées, le Bureau pour la surveillance de la protection des données doit pouvoir vérifier, dans le cas d'une communication au sens de l'alinéa 2, lettre *a*, si les «garanties suffisantes» offrent véritablement une protection appropriée pour la communication de données prévue. Pour vérifier le respect de cette obligation, le Bureau doit être informé des garanties, ce que prévoit l'alinéa 3. La réglementation suit là encore l'article 6, alinéa 3 LPD révisée, mais précise que l'information doit être transmise à temps, à savoir avant la communication des données à l'étranger. Ainsi, l'autorité de surveillance a la possibilité, si cela s'avère nécessaire, de remettre avant la communication des données une recommandation formelle (cf. ch. 2.4.3 supra) ou de réagir de manière informelle, ce qui devrait d'ailleurs être la règle en la matière. Aucune délégation explicite pour la réglementation des détails n'est prévue (cf. à ce sujet l'art. 38 LCPD).

Article 17a (nouveau): Contrôle préalable

Pour l'essentiel, la pratique existante dans le domaine des projets informatiques cantonaux est désormais ancrée à l'article 17a, alinéas 1 et 2. La disposition ne contient cependant que des principes et des notions juridiques indéterminées («un nombre important de personnes», «des risques particuliers», «les modifications importantes») que le Conseil-exécutif devra encore préciser dans le cadre des dispositions d'exécution prévues (cf. commentaires au sujet de l'article 38).

L'alinéa 1 énumère différentes conditions en présence desquelles l'autorité de surveillance peut être consultée. Par obligations particulières de garder le secret (lit. *c*), il faut comprendre les obligations légales spécifiques, telles que celles qui sont prévues par la législation sur les assurances sociales, et non les obligations contractuelles conclues à titre facultatif. En règle générale, le résultat du contrôle préalable et, partant, la prise de position de l'autorité de surveillance n'ont pas le caractère d'une instruction obligatoire. Pour autant que cela s'avère nécessaire, ils prennent la forme d'une proposition visant à améliorer la protection des données. Si l'autorité responsable ne suit pas la proposition, le Bureau pour la surveillance de la protection des données peut émettre une recommandation après la mise en service de l'application informatique. Au cas où celle-ci est rejetée, la procédure au sens de l'article 35, alinéa 4 est ouverte.

Les projets informatiques impliquent généralement des coûts très importants, raison pour laquelle la procédure prévue par l'article 35, alinéa 4 peut s'appliquer, selon l'alinéa 3, dès le stade du contrôle préalable, c'est-à-dire avant même le début d'un traitement des données dans la mesure où l'autorité responsable le souhaite. Il devient ainsi possible d'apporter au besoin une solution contraignante aux éventuelles divergences entre l'autorité responsable et l'autorité de surveillance de manière précoce déjà, avant que des coûts inutiles ne soient engagés.

Le contrôle préalable prévu par l'article 17a s'applique à tous les traitements de données au sens de cette disposition et donc en particulier aux systèmes de traitement des données de la police cantonale. Il convient de réglementer à l'article 52 LPol la relation entre ce contrôle et l'octroi d'une autorisation d'exploitation pour des systèmes de ce type (cf. la proposition de nouvel art. 52, al. 6 LPol). Il n'est pas exclu que des projets de recherche médicale soient également soumis à un contrôle préalable au sens de l'article 17a. Il convient de tenir compte, lors d'un tel contrôle, des charges liées à une éventuelle autorisation au sens de l'article 321bis CPS visant à assurer la protection des données ainsi que d'autres conditions générales.

Article 18: Registre des fichiers

Le droit en vigueur prévoit que la responsabilité de la tenue du registre des fichiers incombe en principe exclusivement à l'autorité de surveillance (art. 34, lit. *a*). L'obligation de l'autorité responsable se limite à l'annonce des fichiers (art. 18, al. 1). Dans les faits, l'autorité de surveillance n'est cependant guère à même d'assumer entièrement une telle responsabilité avant tout parce que c'est l'autorité responsable et non elle-même qui sait quels fichiers existent ou lesquels sont modifiés considérablement (cf. aussi ch. 2.2.4 supra). L'article 18 reformulé tient compte de cela tout en réglementant la question de l'enregistrement des fichiers de manière un peu plus complète et plus précise qu'aujourd'hui.

Des indications fiables et aisément accessibles sur l'ensemble des fichiers permettent d'aider les personnes concernées à sauvegarder leurs droits, tels que le droit de consulter des fichiers, de faire rectifier ou effacer des données personnelles. L'alinéa 1 précise par conséquent expressément que l'autorité de surveillance publie sur Internet le registre des fichiers et le tient à jour. La publication du registre n'est pas formellement prévue par le droit en vigueur, mais du fait des motifs évoqués et de la possibilité pour chaque personne de consulter le registre (art. 20), elle est en principe tout au moins indiquée. Elle devra avoir lieu sur Internet, afin de satisfaire aux exigences actuelles en matière de communication. Par «autorité de surveillance», il s'agit de comprendre, comme toujours dans la loi, tant l'autorité cantonale que les autorités communales de surveillance. Comme l'exprime l'alinéa 1, il conviendra de publier dans le registre de l'autorité cantonale de surveillance les fichiers des autorités cantonales tandis que les autorités communales de surveillance publieront les fichiers établis dans la commune ou la collectivité de droit communal en question.

Le nouvel alinéa 4 réglemente des questions de détail liées à la mise à jour du registre. L'obligation de «gérer», c'est-à-dire d'établir le registre et de le mettre à jour relève désormais avant tout des autorités responsables. La véritable «tenue» du registre continue cependant à incomber, conformément à l'article 21, alinéa 2 de la directive de l'UE, à l'autorité de surveillance qui publie le registre sur Internet. Afin de garantir la fiabilité des informations concernant les fichiers existants, l'autorité de surveillance devra demander aux autorités responsables de suivre un certain nombre de consignes en vue de l'établissement et de la mise à jour des différentes parties du registre, par exemple en mettant à leur disposition des masques informatiques. Un tel système est par exemple appliqué à l'heure actuelle dans le canton de Zurich. Si cela devait s'avérer nécessaire, les détails relatifs à l'enregistrement pourraient être réglementés dans les dispositions d'exécution prévues par l'article 38.

Les prescriptions des alinéas 1 et 4 s'appliquent de toute façon au canton et aux organes des collectivités et établissements ainsi qu'aux personnes de droit privé qui ont été mandatés au sens de l'article 2, alinéa 5, lettre *b*. Par égard envers l'autono-

mie dont jouissent les communes en matière d'organisation et en particulier envers les besoins des collectivités de droit communal de petite taille, l'alinéa 5, lettre *a* permet aux communes, ainsi qu'aux autres collectivités de droit communal, d'adopter dans leurs dispositions relevant du droit de l'organisation des réglementations qui dérogent à l'alinéa 4 et qui permettent par exemple à l'autorité de surveillance de continuer à assumer l'entière responsabilité du registre. Si une commune ne réglemente pas les compétences de manière divergente, l'alinéa 4 lui est également applicable. Vu les motifs précités, les communes peuvent également disposer de la possibilité prévue à l'alinéa 5, lettre *b* et renoncer à la publication du registre sur Internet. En effet, des collectivités de droit communal de petite taille qui ne disposent pas d'un site Internet auraient éprouvé une réelle difficulté à respecter la stricte réglementation de l'alinéa 1. Contrairement à l'alinéa *a,* l'alinéa *b* ne parle pas de «réglementer», ce qui implique qu'il est également possible de renoncer à la publication sur Internet par simple voie d'arrêté.

La nouvelle réglementation de l'alinéa 4 permet de décharger l'autorité de surveillance. Dans ces conditions, il n'est plus vraiment judicieux de lui annoncer les fichiers qui ne doivent pas être enregistrés selon l'alinéa 3. Ce dernier est donc adapté en conséquence.

Article 26: Dispositions applicables

Dans le droit en vigueur, l'article 26 renvoie uniquement à la loi sur la procédure et la juridiction administratives et à la loi du 16 mars 1998 sur les communes (LCo)[24]. Dans le domaine de la protection des données, les mesures prises revêtent souvent la forme de décisions au sens de l'article 49 LPJA, qui peuvent être attaquées dans le cadre d'un recours administratif. Si le traitement des données a lieu dans le cadre d'une procédure civile ou pénale qui est close ou s'il est effectué par la police, en application de l'article 49, alinéa 2 LPol, une décision au sens de l'article 134, alinéa 3 CPC ou de l'article 83, alinéa 2 ainsi que de l'article 217, alinéa 4 CPP est rendue. Celle-ci peut être attaquée selon le droit procédural applicable (CPC, CPP) en vertu du principe selon lequel la compétence en matière de voies de droit (dans le domaine de la protection des données) est régie par celle qui prévaut pour l'affaire au fond (droit civil ou pénal). L'article 26 est précisé à cet égard.

Article 27: Recours contre l'autorité de surveillance

La loi en vigueur n'évoque une compétence décisionnelle formelle de l'autorité de surveillance qu'à l'article 27, «les autorités de surveillance [n'étant] pratiquement autorisées à arrêter des décisions qu'en rapport avec des enregistrements» (rapport du 26 juin 1985 présenté par la Direction de la justice au Conseil-exécutif, à l'intention du Grand Conseil, concernant la loi sur la protection des données, commentaire relatif à l'art. 27). L'article 27 est toutefois resté lettre morte puisqu'il semble que les autorités de surveillance n'aient jamais fait usage de cette compétence.

Au vu de la responsabilité nouvellement réglementée à l'article 18 au sujet du registre des fichiers et des pouvoirs d'intervention particuliers de l'autorité de surveillance prévus par l'article 35, il apparaît indiqué de supprimer sans la remplacer cette disposition qui n'a aucune signification pratique. En relation avec les pouvoirs d'intervention, une compétence décisionnelle formelle de l'autorité de surveillance (cf. ch. 2.4.3 supra) est volontairement abandonnée; par conséquent, le maintien de l'article 27 serait contraire au système.

Article 31: Emolument perçu pour la consultation de données et la communication de renseignements

Le principe de la gratuité en cas de consultation de données et de communication de renseignements que prévoient les dispositions de droit européen est déjà valable dans la pratique, mais il n'est pas expressément formulé dans le droit en vigueur. Il convient donc d'adapter l'article 31 afin qu'il corresponde à ce qui prévaut réellement dans la pratique. D'un point de vue juridique, la rétribution pour la consultation et les renseignements constitue un émolument (administratif), raison pour laquelle il est question, à l'article 31, comme dans le droit actuel, d'émolument. Le principe de la gratuité s'applique selon l'alinéa 1 à la consultation de données et à la communication de renseignements au sens des articles 20 et 21. En cas de recours, il n'est pas exclu que des frais de procédure soient mis à la charge de la partie qui succombe comme le prévoit la loi sur la procédure et la juridiction administratives. Des émoluments ne peuvent cependant être perçus qu'à la condition qu'il existe les bases juridiques nécessaires à cet égard.

L'alinéa 2 habilite le Conseil-exécutif à prévoir pour le canton des dérogations au principe de l'exemption des émoluments. Aujourd'hui déjà, les émoluments sont régis au niveau d'une ordonnance, à savoir l'ordonnance du 22 février 1995 fixant les émoluments de l'administration cantonale (ordonnance sur les émoluments; OEmo)[25]. L'article 31 OEmo prévoit que la consultation du registre des fichiers est gratuite. Selon l'article 32 OEmo, la communication de renseignements et la consultation de données conformément à l'article 21 LCPD sont en principe gratuites. Un émolument peut exceptionnellement être perçu lorsque les renseignements désirés ont déjà été communiqués à la personne requérante dans les douze mois précédant la demande et que cette dernière ne peut justifier d'un intérêt légitime à ce qu'ils lui soient de nouveau communiqués ou lorsque la communication des renseignements demandés occasionne un volume de travail considérable. L'ordonnance sur les émoluments correspond ainsi déjà à la nouvelle réglementation prévue par la loi sur la protection des données et il ne sera par conséquent pas nécessaire de l'adapter.

Le principe de la gratuité s'applique aussi bien au canton qu'aux communes. Le Conseil-exécutif règle les exceptions en vertu de l'alinéa 2 uniquement pour le canton. Dans une volonté de respecter l'autonomie communale, l'alinéa 3 prévoit simplement et de manière générale la possibilité pour les communes et les autres collectivités de droit communal d'édicter des réglementations dérogatoires. Si des

[24] RSB 170.11

[25] RSB 154.21

réglementations communales existantes contreviennent au principe de l'exemption des émoluments au sens de l'alinéa 1, elles devront être adaptées.

Article 32: Autorité cantonale de surveillance en matière de protection des données

L'article 32, alinéa 1 prévoit désormais que la personne déléguée à la protection des données est élue par le Grand Conseil sur proposition du Conseil-exécutif (pour les explications à ce sujet, se reporter au ch. 2.3.3 a) supra). Du fait de l'extension des tâches et des attributions (cf. art. 34 et 35), il n'est plus guère envisageable de prévoir une activité à titre accessoire de la personne occupant cette fonction. Par conséquent, une telle possibilité n'est plus mentionnée explicitement, même si, en principe, elle n'est pas exclue. Il est en revanche désormais clairement précisé, dès l'alinéa 1, que la réglementation de l'article 32 concerne exclusivement l'autorité cantonale de surveillance.

Selon le nouvel alinéa 2, la personne déléguée à la protection des données est élue pour une période de fonction de quatre ans (pour les explications à ce sujet, cf. ch. 2.3.3 b) supra). Le statut juridique de cette personne est régi par les articles 37 et suivants de la loi sur le personnel; il est donc comparable à celui des membres d'autorités judiciaires ou des ecclésiastiques. Un licenciement durant la période de fonction n'entre en ligne de compte qu'en cas de manquements graves (cf. art. 41 s. LPers) et pourrait être examiné dans le cadre d'une procédure judiciaire. Le nouveau statut, en droit du personnel, de la personne déléguée à la protection des données nécessite des adaptations de la loi sur le personnel (cf. ch. 3.2 infra).

L'autorité cantonale de surveillance reste rattachée administrativement à la Direction de la justice, des affaires communales et des affaires ecclésiastiques. Il s'agit là d'un lien purement administratif. L'indépendance de l'autorité de surveillance quant à ses ressources et à son activité doit dans tous les cas être préservée (cf. aussi ch. 2.3.3 d) supra). Le principe de l'indépendance n'est toutefois plus réglementé comme aujourd'hui à l'article 33, mais à l'article 33a nouvellement créé, qui est plus détaillé.

Article 33a (nouveau): Indépendance de l'autorité de surveillance de la protection des données

En raison de son importance, l'indépendance de l'autorité de surveillance doit être réglementée dans un article distinct. Ce principe est d'abord inscrit comme tel à l'alinéa 1, et répond ainsi aux prescriptions du droit européen. L'«autorité de surveillance» au sens de la disposition recouvre aussi bien l'autorité cantonale que les autorités de surveillance des communes et des autres collectivités de droit communal. La deuxième phrase s'inspire de la formulation de la réglementation concernant le Contrôle cantonal des finances, qui figure à l'article 4, alinéa 2 de la loi du 1er décembre 1999 sur le Contrôle des finances (LCCF)[26]. L'indépendance de l'autorité de surveillance suppose par exemple que celle-ci décide elle-même du programme de contrôle, sans subir l'influence du gouvernement ou de l'administration et qu'elle peut exercer librement les pouvoirs d'investigation et d'intervention prévus par l'article 35 ainsi que celui d'ester en justice et d'avertir l'autorité (cf. ch. 2.4.4 supra). Elle doit en particulier également avoir la possibilité de refuser des mandats spéciaux que le pouvoir exécutif ou l'administration veulent lui confier si elle estime que ceux-ci pourraient mettre en péril l'exécution indépendante du programme de contrôle.

Comme mentionné au chiffre 2.3.3 c) supra, les prescriptions des accords de Schengen/Dublin prévoient que l'autorité de surveillance dispose également d'un budget qui lui est propre que le gouvernement et l'administration ne peuvent nullement influencer. Le budget de l'autorité de surveillance en matière de protection des données doit par conséquent être intégré au budget cantonal, ce qui incombe à l'administration. L'alinéa 2 prescrit tout d'abord que la législation sur le pilotage des finances et des prestations s'applique en principe également à l'autorité de surveillance. L'alinéa 3 établit les principes de l'accent mis sur les prestations et sur les coûts selon la NGP, réglemente la procédure d'établissement du plan intégré «mission-financement» et du budget, et prévoit en outre que le Conseil-exécutif peut commenter le budget à l'intention du Grand Conseil. Le Grand Conseil décide en fin de compte dans le cadre de sa souveraineté budgétaire s'il veut mettre à disposition les moyens demandés pour la surveillance de la protection des données. L'alinéa 4 précise clairement que l'autorité de surveillance dispose elle-même des moyens qui lui ont été alloués par le budget. Ces ressources peuvent être affectées à l'engagement de personnel mais aussi à d'autres fins, telles que le paiement de prestations de spécialistes. Dans ce contexte, c'est à dessein qu'on a renoncé à exiger la conclusion d'une convention de prestations telle qu'elle est par exemple prévue à l'article 10 LCCF. Une telle convention contreviendrait en effet au principe de l'indépendance de l'autorité de surveillance.

Le principe de l'indépendance de l'autorité de surveillance au sens de l'alinéa 1 vaut aussi bien pour le canton que pour les communes et les autres collectivités de droit communal. En revanche, les alinéas 2 à 4 sont prévus exclusivement pour le canton et ne peuvent être appliqués aux communes sous cette forme. L'alinéa 5 prévoit en termes généraux que les autorités de surveillance des communes doivent elles aussi bénéficier d'une indépendance en matière de ressources. Les communes devront garantir à leur tour l'indépendance de leur autorité de surveillance en adoptant des réglementations adaptées. Il serait envisageable de créer une réglementation cantonale plus précise, au niveau d'une ordonnance, qui pourrait prévoir par exemple que les autorités communales de surveillance bénéficient des mêmes compétences en matière de dépenses qu'un organe de vérification des comptes, à condition que les communes n'en disposent pas autrement[27].

L'indépendance de l'autorité de surveillance ne doit toutefois pas conduire à une situation qui verrait cet organe se transformer en un «quatrième pouvoir» incontrôlé

[26] RSB 622.1

[27] Cf. à ce sujet l'article 127 de l'ordonnance du 16 décembre 1998 sur les communes (OCo; RSB 170.111)

voire même à un «Etat dans l'Etat». Un tel risque n'existe pas. L'autorité cantonale de surveillance est elle-même soumise à une surveillance conçue de manière adéquate (cf. ch. 3.2 infra, commentaire relatif aux art. 38 et 41 LPers) et doit, en vertu de l'article 37, alinéas 1 et 2, également rendre compte de son activité. La même obligation qui incombe aux organes communaux est régie par les réglementations propres aux communes (cf. art. 37, al. 3). La conduite tant administrative que financière des autorités de surveillance est examinée dans le cadre de la vérification des comptes.

Article 34: Tâches de l'autorité de surveillance

L'article 34, alinéa 1 énumère sous une forme concentrée les tâches qui incombent à l'autorité de surveillance. Là encore, cette disposition s'applique aussi bien à l'autorité de surveillance cantonale que communale. La lettre *a* est rédigée sous une nouvelle forme, la lettre *k* représente une extension de l'actuelle lettre *g*. Les lettres *c, d* et *n* sont nouvelles. Les lettres *g* et *h* correspondent à l'actuelle lettre *e.* Les autres dispositions prévues aux lettres *b*, *e, f, i, l* et *m* correspondent de façon littérale à la réglementation aujourd'hui en vigueur (lit. *b, c, d, f*, *h* et *i*).

La lettre *a* concorde avec l'alinéa 1 de l'article 18 qui réglemente l'enregistrement des fichiers. La tournure «tient à jour [...] au sens de l'article 18» indique que dans ce contexte-là, les obligations n'incombent pas uniquement à l'autorité de surveillance, mais aussi aux autorités responsables (cf. à ce sujet les commentaires relatifs à l'art. 18). La lettre *c* renvoie aux contrôles préalables nouvellement réglementés à l'article 17a. La lettre *d*, quant à elle, respecte le principe qui est en fait déjà en vigueur et qui prévoit que des requêtes de personnes intéressées doivent être traitées au même titre que des dénonciations à l'autorité de surveillance au sens de l'article 101 LPJA. Cette réglementation expresse a surtout été introduite en vue du nouvel alinéa 2. La lettre *k*, dont la formulation est nouvelle comprend désormais non seulement les textes législatifs mais aussi d'autres mesures telles que des moyens de garantir la sécurité informatique, des enquêtes, la conception et la modification de processus comme la délivrance de certificats électroniques, etc. La lettre *n* précise enfin l'obligation de collaborer avec d'autres autorités de surveillance et d'accorder l'entraide administrative (cf. à ce sujet ch. 2.4.5 supra).

Le nouvel alinéa 2 prescrit que l'autorité de surveillance informe dans les cas cités les personnes intéressées de l'examen effectué sur la base des requêtes prévues à l'alinéa 1, lettre *d* même si celles-ci n'en font pas expressément la demande. Conformément aux prescriptions des accords de Schengen/Dublin (cf. ch. 2.4.1 supra), cette réglementation va au-delà de la disposition de portée générale de l'article 101, alinéa 2 LPJA, qui prévoit que des informations sur la liquidation d'une dénonciation à l'autorité de surveillance ne sont fournies que sur demande.

Article 35: Méthode de travail de l'autorité de surveillance et procédure

L'article 35 réglemente à l'alinéa 3 complété et aux nouveaux alinéas 4 et 5 les pouvoirs d'intervention de l'autorité de surveillance conformément à la solution prévue par la variante b) décrite au chiffre 2.4.3 supra. L'alinéa 6 correspond à l'actuel alinéa 4.

L'alinéa 3 reprend la réglementation actuelle mais prévoit en outre que l'autorité de surveillance doit émettre sa recommandation sous la forme d'une proposition motivée. Elle peut ainsi établir elle-même pour l'essentiel, même sans disposer de compétence décisionnelle formelle, l'objet de la décision qui devra, le cas échéant, être rendue par l'autorité compétente (al. 4), ainsi que d'une éventuelle procédure de recours ultérieure au sens de l'alinéa 5 (la compétence actuelle permettant de rendre ses propres décisions en relation avec les enregistrements de fichiers est supprimée; cf. commentaire relatif à l'art. 27). Une telle réglementation évite que les autorités responsables, qui disposent d'une certaine marge d'appréciation quant à l'application de la recommandation, n'accordent pas suffisamment d'importance aux aspects de la protection des données. Parallèlement, une proposition munie d'une motivation peut apporter une aide bienvenue, notamment aux services peu versés dans les procédures administratives, lorsqu'il s'agit de prononcer une décision. L'autorité de surveillance devra motiver sa recommandation de manière telle que le service concerné, même s'il ne dispose pas d'une expérience en la matière, soit à même d'examiner la question et, le cas échéant, de statuer dans le délai prévu à l'alinéa 4 sur le refus (partiel) des recommandations.

Si l'autorité traitant les données ne suit pas la proposition motivée de l'autorité de surveillance, elle doit, comme le prévoit l'alinéa 4, rendre une décision susceptible d'être attaquée. Il s'agira en règle générale d'une décision au sens de l'article 49 LPJA. Mais si le traitement des données a lieu dans le cadre d'une procédure close civile ou pénale ou qu'il relève de la police selon l'article 49, alinéa 2 LPol, il convient, conformément à la réglementation actuelle en matière de demande de consultation de dossier, de rendre une décision au sens de l'article 134, alinéa 3 CPC ou des articles 83, alinéa 3 ou 217, alinéa 4 CPP. Il paraît approprié de fixer un délai adapté pour la décision susceptible d'être attaquée pour éviter de donner la possibilité à une autorité opposée à la recommandation de reporter la procédure indûment. L'alinéa 4 prévoit le délai de trente jours qui est habituel pour les procédures administratives. Une telle réglementation permet d'assurer que des divergences, le cas échéant, puissent être liquidées par une décision à caractère obligatoire dans les meilleurs délais.

L'alinéa 5 habilite l'autorité de surveillance à attaquer la décision. La procédure est régie par le droit procédural applicable (cf. art. 26 et les commentaires y relatifs) bien qu'il existe dans tous les cas la possibilité qu'une instance judiciaire statue, si nécessaire, sur des divergences résiduelles. En cas d'applicabilité de la loi sur la procédure et la juridiction administratives, cela signifie que tout comme cela se fait lors d'un recours d'un particulier, l'opportunité de la disposition peut en principe faire l'objet d'un examen dans une procédure de recours administratif (art. 66, al. 1, lit. *c* LPJA). Sur ce point, l'instance de recours doit cependant régulièrement faire preuve de réserve dans le cas de décisions communales afin de respecter notamment l'autonomie communale. Il convient également de tenir compte du fait qu'en vertu de l'alinéa 3, l'autorité de surveillance peut seulement demander de «remédier

à des irrégularités et de combler des lacunes», en engageant une procédure de recours à cet égard. Des mesures qui sont en soi convenables, même si elles sont susceptibles d'être encore améliorées, ne constituent aucune irrégularité ou lacune au sens de l'alinéa 3. Comme l'exprime l'article 34, alinéa 1, lettre *g*, dans sa nouvelle formulation, les simples propositions d'amélioration font partie de l'activité générale de conseil de l'autorité de surveillance qui, en principe, ne débouche pas sur une recommandation formelle au sens de l'article 35, alinéa 4. Dans la pratique, une importance limitée est accordée à l'examen de la seule opportunité des décisions au sens de l'alinéa 4.

Article 37: Obligation de rendre compte

Un nouveau point évoqué à l'article 37 est celui du rapport que l'autorité de surveillance doit soumettre au Conseil-exécutif. Ce sont surtout le Grand Conseil et le Conseil-exécutif qui devront en prendre connaissance. Ils ne peuvent agir que dans le cadre de leurs compétences, par exemple en vue de l'édiction d'une nouvelle réglementation, le cas échéant, dans la loi ou dans l'ordonnance (art. 38). Une action directe exercée sur l'activité de la personne déléguée à la protection des données irait à l'encontre du principe de l'indépendance totale dont doit jouir l'autorité de surveillance.

Article 38: Dispositions d'exécution

Tout comme la réglementation actuelle, l'article 38 habilite le Conseil-exécutif, de manière générale, à édicter des dispositions d'exécution. On peut songer notamment aux détails liés, le cas échéant, à l'enregistrement de fichiers (art. 18) et à d'autres prescriptions plus précises sur le contrôle préalable au sens de l'article 17a. Il est prévu de réglementer par voie d'ordonnance les prescriptions de forme générale et abstraite relatives aux projets informatiques qui, à l'heure actuelle, font l'objet d'arrêtés du Conseil-exécutif. Le domaine de la sécurité informatique étant soumis à des changements techniques rapides, il semble adéquat que le Conseil-exécutif puisse, lorsque cela s'avère nécessaire, également déléguer la réglementation de certains sujets précis à des organes subordonnés. L'article 38 contient la base légale nécessaire à cet égard prévue par l'article 69, alinéa 3 ConstC. Du point de vue de son contenu, il correspond à la réglementation de portée générale de l'article 43 de la loi du 20 juin 1995 sur l'organisation du Conseil-exécutif et de l'administration (loi d'organisation, LOCA)[28]. Selon l'article 43, alinéa 2 LOCA, les offices de l'administration cantonale ne sont pas habilités à édicter des ordonnances au sens juridique du terme, mais uniquement ce que l'on nomme des ordonnances administratives, c'est-à-dire des instructions valables de manière interne à l'administration.

3.2 Autres actes législatifs

Articles 38 et 41 de la loi sur le personnel

Etant désormais élue pour une période de fonction (art. 32, al. 2 LCPD), la personne déléguée à la protection des données dans le canton ne dispose plus du statut d'employé au sens de l'article 3, alinéa 2 LPers. Elle accomplit les tâches conformément à l'article 33a, alinéa 1 LCPD de manière indépendante et ne peut pas, par conséquent, du point de vue du droit du personnel, être soumise à la surveillance d'un service administratif qui lui est hiérarchiquement supérieur. Pour des principes relevant de l'Etat de droit, on ne peut toutefois envisager un service qui ne serait soumis à aucun contrôle. Par conséquent, il convient de réglementer, en tenant compte de l'indépendance nécessaire, la surveillance et en particulier la compétence en matière de révocation.

Le statut juridique de la personne déléguée à la protection des données peut être comparé à celui du chancelier ou du secrétaire du parlement qui, en tant que membre d'autorité à titre principal au sens de l'article 3, alinéa 4 LPers, est également élu par le Grand Conseil pour une période de fonction. La surveillance exercée sur la personne déléguée est par conséquent réglementée sur le modèle de la solution qui s'applique à ces personnes. Selon l'article 38, alinéa 1, lettre *c* LPers, l'autorité de surveillance est la Commission de haute surveillance qui, au sens de l'article 41, alinéa 4, lettre *c* LPers, est également compétente, le cas échéant, pour proposer la révocation. La décision concernant la révocation est de la compétence du Tribunal administratif (art. 41, al. 1 et 2 LPers). Cette réglementation permet de tenir compte de l'exigence de l'indépendance de l'autorité de surveillance de la protection des données à l'égard du gouvernement et de l'administration.

Article 23 de la loi sur la procédure et la juridiction administratives: consultation du dossier

En raison de l'extension du champ d'application de la loi sur la protection des données aux procédures administratives pendantes, à l'article 4, alinéa 2, lettre *c* LCPD, il convient d'adapter l'article 23, alinéa 3 LPJA en conséquence. La formulation «la loi du 19 février 1989 sur la protection des données s'applique *en sus*» exprime le fait que la loi sur la procédure et la juridiction administratives s'applique bien entendu également à de telles procédures pour autant que le domaine spécifique du traitement de données ne soit pas concerné (cf. art.1 LPJA.) Quant à la référence aux procédures closes mentionnées actuellement à l'article 23, alinéa 3 LPJA, elle est supprimée. Cette loi ne concerne que les procédures pendantes et ne réglemente en principe pas les procédures closes, auxquelles seule s'applique selon le droit actuel la loi sur la protection des données. Il est donc possible de renoncer à la réglementation actuelle dans la loi sur la procédure et la juridiction administratives. Cette suppression ne modifie en rien la situation juridique matérielle en ce qui concerne les procédures closes.

[28] RSB 152.01

Article 52 de la loi sur la police: systèmes de traitement des données de la Police cantonale

Même si à l'avenir, le contrôle préalable au sens de l'article 17a LCPD doit jouer un rôle de premier plan pour les systèmes informatiques de la Police cantonale, il apparaît justifié de conserver l'instrument de l'autorisation d'exploitation à l'article 52 LPol. Le Conseil-exécutif assume ainsi une part de la responsabilité globale en matière de système de traitement des données de la police. Toutefois, afin d'éviter des doublons, il convient de coordonner la procédure concernant le contrôle préalable au sens du droit de la protection des données et celle relative à l'autorisation d'exploitation. Par conséquent, le nouvel alinéa 6 de l'article 52 LPol prévoit que le contrôle préalable intervient avant la remise de l'autorisation d'exploitation.

Article 39a de la loi sur la santé publique: consultation et remise du dossier médical

La loi sur la santé publique (LSP)[29] prévoit actuellement, à l'article 39a, alinéa 2 que lors de la consultation de dossiers médicaux, les copies effectuées peuvent être facturées au prix coûtant. A l'avenir, une telle possibilité devra demeurer l'exception, raison pour laquelle il y a lieu d'adapter cette disposition. La mention «la législation applicable, en particulier celle concernant la protection des données» est de portée générale car le champ d'application de la loi sur la santé publique s'étend aussi bien au traitement de patients dans des institutions publiques et privées que par des professionnels de la santé exerçant à titre privé, ce qui suppose qu'en fonction du cas particulier, le droit cantonal sur la protection des données, la réglementation de droit fédéral ou, le cas échéant, une autre prescription légale peut s'appliquer.

4. Répercussions

4.1 Répercussions sur les ressources financières et humaines

Il n'est pas facile d'évaluer les répercussions de la révision sur les ressources humaines et financières. A l'heure actuelle, le Bureau cantonal pour la surveillance de la protection des données emploie un délégué à plein temps (classe de traitement 24). Pour les tâches de secrétariat, ce dernier peut recourir aux chancelleries de l'Office juridique et du Secrétariat général de la JCE, à hauteur de 20 à 40 pour cent. Il dispose en outre de la possibilité de confier des mandats aux juristes stagiaires de l'Office juridique de la JCE. Enfin, le Conseil-exécutif accorde au délégué un montant annuel de 130 000 francs (un pour mille des coûts d'exploitation informatique annuels) pour des examens de la protection des données dans son domaine d'action.

Même après la révision de la loi sur la protection des données, il reviendra avant tout aux unités propres à l'administration, c'est-à-dire en premier lieu aux services juridiques des Directions de conseiller les services cantonaux. Le délégué ou la déléguée à la protection des données devra toutefois assumer des tâches et des compétences élargies dans le cadre de la nouvelle réglementation. Les pouvoirs d'investigation et d'intervention réglementés à l'article 35 LCPD révisé entraîneront notamment un travail plus important. Il s'agira également d'apporter un soutien accru aux autorités de surveillance des collectivités de droit communal. L'autorité de surveillance cantonale devra être organisée de manière à pouvoir également procéder aux contrôles et aux interventions efficaces qui sont prescrits et dotée de ressources à cet égard. Elle devra notamment assurer le suivi du traitement des données dans le cadre du Système d'information de Schengen SIS II (informations policières) exploité par 28 Etats européens comptant 450 millions d'habitants, ce qui présuppose des connaissances juridiques et informatiques adéquates. Comme mentionné, les ressources à ce sujet devront être autorisées dans le cadre d'un budget présenté séparément. Les exigences supplémentaires que posent les accords de Schengen/Dublin vont certainement impliquer à l'avenir des charges plus élevées. En l'état actuel des connaissances, on peut partir du principe qu'il faudra un poste supplémentaire de l'ordre de 80 à 100 pour cent pour un collaborateur ou une collaboratrice scientifique et un autre de 50 pour cent pour le secrétariat, ce qui entraîne une augmentation des charges annuelles de personnel de 250 000 francs environ (au sujet du financement du poste dû au transfert de l'autorité de surveillance de la protection des données des hôpitaux au délégué cantonal, cf. ch. 2.3.4 supra). La publication du registre des fichiers sur Internet implique des coûts uniques estimés à 60 000 francs, dus à la création des moyens informatiques ad hoc. Les frais périodiques pour l'exploitation du registre s'élèveront à moins de 10 000 francs par an; il ne s'agit pas là à proprement parler de coûts supplémentaires. La loi sur la protection des données en vigueur prévoit déjà un mandat de tenue du registre, qui n'a cependant jamais été mis en œuvre.

4.2 Répercussions sur les communes

En raison de la proposition de refus d'une cantonalisation de la surveillance de la protection des données, l'autonomie des communes en matière d'organisation ne devrait pas être restreinte. S'agissant de l'indépendance et de l'activité de l'autorité de surveillance, l'association aux accords de Schengen/Dublin et le Protocole additionnel posent toutefois des exigences accrues, imposent des réglementations et, dans une certaine mesure, des charges supplémentaires. Quant à l'application des prescriptions légales, les communes doivent, comme cela a été relevé, disposer d'un soutien sous une forme appropriée (ISCB, adaptation du règlement type sur la protection des données).

5. Résultat de la procédure de consultation

Une procédure de consultation a été menée au sujet du présent projet de loi entre début mars et début juin 2007 et a donné lieu à 43 prises de position. Le principe d'une révision de la loi sur la protection des données n'est pas contesté et le projet a généralement rencontré un écho positif. Suite à la procédure de consultation, le projet a donc uniquement subi des modifications mineures.

[29] RSB 811.01

Pour le PS, certains points, notamment celui de la protection des données dans les communes, ne sont pas suffisamment développés. Ses propositions dépassent toutefois le cadre de ce qu'exige une adaptation pragmatique aux prescriptions de l'UE et ne doivent donc être examinées que lors d'une éventuelle révision complète du droit de la protection des données. Le PRD estime quant à lui que la compétence en matière de financement et de budgétisation qui doit être accordée à la personne déléguée à la protection des données est trop étendue. Afin de clarifier les choses, il est désormais précisé dans le présent rapport que le Grand Conseil conserve sa souveraineté dans le domaine budgétaire et qu'il n'existe aucune obligation de reprendre, sans le modifier, le budget et le plan financier présentés par l'autorité de surveillance.

Au sujet de l'article 14a (échange de données avec l'étranger), plusieurs participants à la procédure de consultation (PRD, UDC, Jeunes radicaux et Direction des finances) ont critiqué les libertés prises par rapport au droit fédéral. Une telle objection est justifiée, puisque dans ce domaine en particulier, une solution conforme au droit fédéral paraît adéquate. L'article 14a a donc été reformulé en s'inspirant davantage de l'article 6 de la loi fédérale sur la protection des données. En ce qui concerne l'alinéa 3 de l'article 14a (obligation d'informer avant la communication de données personnelles à l'étranger), la version d'origine est conservée, puisque cela n'est pas uniquement dans l'intérêt de la personne concernée, mais aussi de l'autorité compétente.

En ce qui concerne l'article 31, un certain nombre de représentants des milieux consultés (PRD, Jeunes radicaux, commune d'Ittigen) remettent en cause le principe de l'exemption d'émoluments. A la lumière des prescriptions de l'UE, une réglementation opposée n'aurait guère de chance d'être approuvée dans la perspective d'une évaluation effectuée par l'UE.

L'article 33a (indépendance de l'autorité de surveillance) a suscité quelques réactions de la part de participants à la procédure de consultation qui souhaitent des prescriptions plus claires. Les communes seront informées en temps voulu et de manière détaillée sur les nouvelles exigences, par l'intermédiaire d'une communication dans l'ISCB.

Les associations communales et la ville de Langenthal ont demandé que dans les procédures de recours, le pouvoir d'examen soit limité à la conformité au droit des décisions communales (art. 35, al. 5). Il convient à cet égard de relever qu'une procédure de recours émanant de l'autorité de surveillance peut porter uniquement sur la volonté de «remédier à des irrégularités et de combler des lacunes» (al. 3). Des mesures appropriées qui pourraient, le cas échéant, être encore légèrement améliorées, ne constituent pas des irrégularités ou des lacunes au sens de l'article 35, alinéa 3. Dans la pratique, l'examen de la seule opportunité de décisions au sens de l'alinéa 4 n'aura donc qu'une importance limitée. Le présent rapport a été adapté en conséquence.

Le projet contient enfin une modification de la loi sur le personnel qui ne figurait pas encore dans la version envoyée en procédure de consultation. Celle-ci permet de réglementer la surveillance qui doit être exercée sur la personne déléguée à la protection des données dans le respect de l'indépendance dont elle doit pouvoir disposer.

6. Proposition

Vu les commentaires qui précèdent, le Conseil-exécutif propose au Grand Conseil d'approuver les présentes modifications.

Berne, le 17 octobre 2007

Au nom du Conseil-exécutif,

le président: *Gasche*
le chancelier: *Nuspliger*

Complément au rapport du Conseil-exécutif du 17 octobre 2007 concernant la modification de la loi sur la protection des données

Article 85a de la loi sur le pilotage des finances et des prestations

Etant donné qu'il ne conclut aucune convention de prestations avec le Conseil-exécutif, le Bureau pour la surveillance de la protection des données ne répond pas à toutes les exigences d'une unité NOG et tient par conséquent un compte spécial conformément à l'article 36, alinéa 1 LFP. En raison de l'interdiction qu'a le gouvernement d'exercer de l'influence, il n'est cependant pas admissible que la manière dont le Bureau pour la surveillance de la protection des données tient sa comptabilité soit réglementée par une ordonnance du Conseil-exécutif. Par conséquent, l'article 36, alinéa 2 n'est pas applicable. Il convient donc, comme cela est prévu pour les autorités judiciaires (art. 85), d'intégrer à la loi une disposition prévoyant que le Grand Conseil règle les structures comptables ainsi que la tenue des comptes par voie de décret.

Berne, le 30 janvier 2008

Au nom du Conseil-exécutif,

le président: *Gasche*
le chancelier: *Nuspliger*