LIBERTÉ ET PATRIE

XXX 2006
AVANT PROJET
APL

EXPOSE DES MOTIFS ET PROJET DE LOI

- sur la protection des données personnelles
- modifiant la loi du 24 septembre 2002 sur l'information
- modifiant la loi du 15 septembre 1999 sur la statistique cantonale

1. INTRODUCTION

1.1 Contexte

1.1.1 Constitution cantonale du 14 avril 2003

La nouvelle Constitution cantonale du 14 avril 2003 (Cst-VD) garantit à tout être humain la liberté personnelle, notamment l'intégrité physique, l'intégrité psychique et la liberté de mouvement (article 12 alinéa 2 Cst-VD).

Elle contient, dans son catalogue des droits fondamentaux, une disposition relative à la protection de la sphère privée et des données personnelles. Conformément à l'article 15 Cst-VD, toute personne a droit au respect et à la protection de sa vie privée et familiale, de son domicile, de sa correspondance et des relations établies par les télécommunications. L'alinéa 2 précise que toute personne a le droit d'être protégée contre l'utilisation abusive des données qui la concernent. Ce droit comprend : a) la consultation de ces données ; b) la rectification de celles qui sont inexactes ; c) la destruction de celles qui sont inadéquates ou inutiles.

Cette disposition s'inspire des garanties énoncées à l'article 13 de la Constitution fédérale du 18 avril 1999 et plus particulièrement, s'agissant de la protection des données personnelles, à son alinéa 2. Le droit à la protection contre l'usage abusif de données personnelles existait cependant avant d'être ancré dans la Constitution fédérale, puisqu'il découle de la liberté personnelle et de l'article 8 de la Convention Européenne des droits de l'Homme (CEDH). Il n'existait toutefois de manière explicite qu'au niveau de la législation, en particulier dans la loi fédérale sur la protection des données du 19 juin 1992[1]. La nécessité de « constitutionnaliser » ce droit est apparue à l'époque de la société d'information et des atteintes potentielles qu'elle représente.

Selon le Commentaire de la Constitution cantonale, le droit de maîtrise des données que tout organisme public peut accumuler sur un individu, notamment grâce à la tenue de fichiers, est garanti par l'article 15 alinéa 2 Cst-VD.

Conformément à l'article 38 Cst-VD les droits fondamentaux ne peuvent être restreints que si une base légale le prévoit (lorsque la restriction est grave, une loi est requise), si un intérêt public ou la protection d'un droit fondamental le justifient. En outre, cette atteinte doit être proportionnelle au but visé.

---

[1] LPD, RS 235.1

1.1.2 Droit communautaire

Le droit communautaire contient plusieurs dispositions applicables à la protection des données. En voici les principales.

Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108)

La Convention STE n° 108[2] est un instrument permettant notamment l'harmonisation des législations nationales afin d'assurer un niveau élevé de protection des données dans le cadre de la libre circulation des informations transfrontières. Elle concrétise les articles 8 et 10 de la CEDH, ratifiée par la Suisse le 28 novembre 1974. La Suisse a ratifié la Convention STE n° 108, le 2 octobre 1997.

En vertu de l'article 4 de la Convention, chaque Etat partie doit prendre les mesures nécessaires pour concrétiser les principes fondamentaux énoncés aux articles 5 à 11 de la Convention, soit dans une loi, soit dans des dispositions juridiques adéquates. Cette obligation incombe dès lors non seulement à la Confédération, mais également aux cantons[3].

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 (Protocole additionnel)

Les Etats parties à la Convention STE n° 108 ont édicté un Protocole additionnel, qui a été présenté par le Conseil fédéral à l'approbation de l'Assemblée fédérale, conjointement au projet de révision de la LPD[4]. L'article 1 du Protocole additionnel prescrit que « chaque partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le Présent Protocole ». Selon ce même article, ce contrôle doit être effectué en « toute indépendance » (article 1 al. 3).

L'adhésion de la Suisse au Protocole d'accord entraîne notamment des conséquences au niveau des cantons, puisqu'ils doivent y adapter leur législation. Cette adaptation a trait aux conditions de transfert des données à

---

[2] RS 0.235.1
[3] FF 1996 I 706
[4] FF 2003, p. 1977

caractère personnel vers un autre Etat, de même qu'à celles relatives à l'indépendance et aux pouvoirs de l'autorité de surveillance[5].

Accords Schengen et Dublin

Le 5 juin 2005, le Souverain a approuvé l'association de la Suisse aux Accords conclus entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (Accord de Schengen[6]), ainsi que l'Accord entre la Confédération suisse et la Communauté européenne relatif aux critères et aux mécanismes permettant de déterminer l'Etat responsable de l'examen d'une demande d'asile introduite dans un Etat membre ou en Suisse (Accord de Dublin[7]), signés le 26 octobre 2004 et adoptés par les Chambres fédérales le 17 décembre 2004[8].

La transcription de ces Accords, notamment en matière de protection des données, relève à la fois de la Confédération et des cantons.

Ces Accords ont des incidences directes en matière de protection des données, qui sont régies par différentes dispositions légales communautaires. Ces normes sont différentes selon les domaines de coopération considérés. En effet, les actes législatifs et les mesures constituant l'acquis de Schengen ont été intégrés dans l'édifice juridique de l'UE[9] qui, depuis le Traité de Maastricht[10], comporte trois piliers :

– le *premier pilier*, qui est formé par la CE (Traité instituant la Communauté européenne, TCE) ;

---

[5] FF 2003, p. 1959

[6] L'*Accord de Schengen* favorise la libre circulation des personnes grâce à la suppression des contrôles de personnes aux frontières internes. Un renforcement de la sécurité interne est assuré par les contrôles aux frontières externes de l'espace Schengen, et par une coopération transfrontalière en matière de justice et police renforcée entre les Etats Schengen. La Suisse adhère au système d'information de Schengen (SIS), une base de données informatisée contenant plusieurs dizaines de millions des renseignements sur les personnes et les objets recherchés.

[7] L'*Accord de Dublin* règle l'association de la Suisse à la directive de l'Union Européenne sous l'abréviation de Dublin II, ainsi qu'à l'Eurodac[7]. Grâce à cette base de données, dans laquelle sont enregistrées les empreintes digitales des requérants d'asile, une personne ayant déposé plusieurs demandes d'asile peut être identifiée et reconduite dans le pays de premier asile.

[8] FF 2004, p. 6709

[9] Protocole intégrant l'acquis de Schengen dans le cadre de l'Union européenne (1997) (Protocole sur Schengen, JO n° C 340 du 10.11.1997, p. 93).

[10] Traité du 7.2.1992 sur l'Union européenne (JO n° C 191 du 29.7.1992, p. 1), en vigueur depuis le 1.11.1993.

– le *deuxième pilier*, qui comprend les dispositions concernant la politique étrangère et de sécurité commune (articles 11 à 28 du Traité sur l'Union européenne, TUE) ;

– le *troisième pilier*, qui regroupe les dispositions relatives à la coopération policière et judiciaire en matière pénale[11].

La Directive européenne 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 des données (Directive 95/46/CE)[12], s'applique dans le premier pilier. Aussi, selon le Message, les cantons devront transposer la Directive 95/46/CE dans les dispositions de droit cantonal régissant les différents domaines relevant du premier pilier précité[13].

Directive 95/46/CE

La Directive 95/46/CE régit le traitement de données à caractère personnel automatisé et non automatisé (article 3 paragraphe 1). Elle contient notamment des règles applicables à la qualité des données (article 6), à la légitimation des traitements de données (article 7), à l'information de la personne concernée, à l'obligation de notifier les traitements à une autorité de contrôle (articles 14 et ss.), ainsi qu'à la surveillances des données, qui doit être assurée par une autorité indépendante (article 28).

Cette Directive concrétise et élargit les principes contenus dans la Convention STE n° 108[14].

Comme indiqué ci-dessus, la Directive 95/46/CE s'applique à certains domaines relevant des Accords de Schengen et de Dublin (soit le premier pilier). Or, l'application sectorielle de la Directive aux seuls domaines concernés risque de conduire à une situation insatisfaisante du point de vue de la sécurité du droit, dans la mesure où l'on pourrait se retrouver, selon la nature des données en question, avec deux régimes différents en matière de protection des données : d'un côté, la Directive 95/46/CE, de l'autre le droit cantonal sur la protection des données. Aussi l'option consistant à adapter le présent avant-projet de loi, dans la mesure du possible, au droit communautaire, y compris à la Directive 95/46/CE, a-t-elle été choisie. Cela vaut en particulier pour les définitions,

---

[11] Message 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»), p. 5732
[12] JO n° L 281 du 23 novembre 1995, p. 31
[13] Message 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»), p. 5799
[14] ibid.

certains droits des personnes concernées et l'autorité chargée de la protection des données.

1.2 Situation actuelle

1.2.1 Confédération

La loi fédérale sur la protection des données personnelles du 19 février 1992 s'applique aux données traitées par la Confédération et par les privés. En effet, si la Constitution fédérale contient un article sur la protection des données (article 13), elle n'attribue pas à la Confédération de compétence constitutionnelle en la matière. Aussi la loi fédérale ne s'applique-t-elle qu'au traitement des données par les organes de la Confédération et par les personnes privées (article 2 alinéa 1 lettres a et b LPD). Elle fixe cependant également des règles applicables aux cantons lorsque ces derniers exécutent le droit fédéral (article 37 LPD).

La LPD a fait récemment l'objet de modifications, d'une part suite au dépôt de deux motions parlementaires[15], d'autre part pour rendre le droit suisse compatible avec le Protocole additionnel, adopté par le Conseil fédéral le 17 octobre 2002[16]. Ces modifications ont suscité de nombreuses discussions au niveau des Chambres fédérales ; elles ont finalement été adoptées[17]. Bien que ces modifications ne tiennent pas compte de celles rendues nécessaires par l'acceptation des Bilatérales II, en particulier des Accords de Schengen et de Dublin, elles se conforment, dans une certaine mesure, aux exigences posées par ces Accords, notamment en matière d'obligation d'informer (nouvel article 4 alinéa 4 et nouvel article 7 LPD). Alors que le Message évoque la possibilité de proposer d'autres modifications, voire de procéder à une refonte de la loi à la suite de l'adhésion de la Suisse aux Bilatérales II, il a été décidé que cela était prématuré[18]. Les autorités fédérales attendent le résultat de l'examen qui sera effectué, probablement en 2006, par les pays membres de Schengen afin de déterminer les besoins ou non d'adaptation de la loi fédérale.

---

[15] Motion de la Commission de gestion du Conseil des Etats le 21 décembre 1999 (motion 98.3529 du 17 novembre 1998, « Liaisons «online». Renforcer la protection pour les données personnelles ») et motion de la Commission des affaires juridiques du Conseil des Etats (motion 00.3000 du 28 janvier 2000, « Renforcement de la transparence lors de la collecte des données personnelles »).

[16] Ce Protocole revêt deux aspects: d'une part il s'agit d'aller vers une harmonisation du fonctionnement et des compétences des autorités de contrôle, d'autre part d'éviter que des transferts de données à destination d'Etats ou d'entités tiers n'amènent à contourner la législation de l'Etat d'origine partie à la Convention STE n° 108 (Message du Conseil fédéral du 19 février 2003, pp. 1927 et ss.).

[17] FF 2006, p. 3421 ; le délai référendaire court jusqu'au 13 juillet 2006

[18] Message du Conseil fédéral du 19 février 2003 (FF 2003, pp. 1915 et ss), p. 1930

L'une des modifications de la LPD concerne l'article 37, qui a trait à l'exécution du droit fédéral par les cantons. Cette nouvelle disposition prévoit que certaines dispositions de la LPD s'appliquent au traitement des données par les autorités cantonales, à moins que la législation cantonale applicable à la protection de données n'assure un « niveau de protection adéquat ». Par « niveau adéquat », il faut comprendre un niveau équivalent à celui offert par la Convention STE no 108 qui, comme chaque accord international conclu par la Confédération, lie également les cantons[19].

La LPD a également été modifiée suite à l'adoption de la loi fédérale sur le principe de la transparence dans l'administration (LTrans)[20], entrée en vigueur le 1er juillet 2006. Cette loi attribue notamment au Préposé fédéral à la protection des données, qui devient le Préposé fédéral à la protection des données et à la transparence, un rôle de médiation dans le cadre de l'accès aux documents officiels. Il assume également la fonction d'organe de conseil auquel peuvent s'adresser les autorités et particuliers afin d'obtenir des renseignements sur les modalités d'accès aux documents officiels. Les autres modifications concernent les documents officiels renfermant des données personnelles, qui font l'objet de dispositions particulières.

1.2.2 Cantons

La protection des données découle des droits constitutionnels ; les cantons doivent donc assurer que le traitement des données satisfait aux exigences posées par la Constitution. En outre, certaines tâches assumées par les cantons relèvent du droit fédéral ; par conséquent, une uniformité entre les règles applicables au traitement des données par les autorités fédérales d'une part, et par les autorités cantonales d'autre part, est souhaitable.

A l'heure actuelle, la quasi totalité des cantons suisses s'est dotée de dispositions légales sur la protection des données[21] ou, à tout le moins, sur les informations traitées automatiquement par ordinateur (*Genève*, loi du 17 décembre 1981 sur les informations traitées automatiquement par ordinateur), ou sur la protection de la personnalité (*Neuchâtel*, loi du 3 novembre 1982 sur la protection des la personnalité). Certains cantons ont entamé des démarches en vue de modifier leur législation applicable à la protection des données (*Genève*[22], *Neuchâtel*). En raison des liens étroits

[19] Message du Conseil fédéral du 19 février 2003, p. 1957
[20] FF 2004, p. 6807
[21] Appenzell Rhodes-intérieures, 2000; Bâle campagne, 1991, Bâle ville, 1992, Berne, 1986; Fribourg, 1994 ; Jura, 1986 ; Lucerne, 1990 ; Schaffhouse, 1994 ; Valais, 1984; Tessin, 1987 ; Thurgovie, 1987; Zoug, 2000; Zurich, 1993
[22] Cf. projet de loi du Conseil d'Etat du 7 juin 2006 (PL 9870)

existant entre la protection des données et la transparence de l'administration, ces deux domaines font parfois l'objet d'une seule et même loi ; tel est par exemple le cas du canton de *Soleure (*Informations- und Datenschutzgesetz, du 21 février 2001). Les cantons de *Genève* et de *Zurich* pourraient suivre la même voie. Le Canton de Neuchâtel a lui opté pour deux lois distinctes ; cela étant, un seul Préposé sera chargé de la surveillance des deux lois.

1.2.3 Canton de Vaud

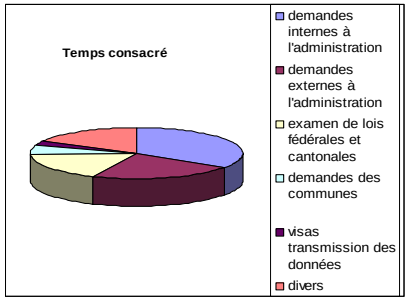
Le Parlement vaudois a adopté en 1981 une loi sur les fichiers informatiques et la protection des données (LIPD)[23]. Cette loi a été élaborée lors de la généralisation de l'informatique, soit du traitement informatisé des informations. Son champ d'application s'étend donc aux fichiers informatiques ou aux fichiers manuels exploités en liaison avec une installation de traitement informatisé de données, que l'Etat, les communes, les établissements ou corporations de droit public exploitent directement ou par l'intermédiaire de tiers (article 2 alinéas 1 et 2 LIPD). La LIPD est précisée par les Directives du Conseil d'Etat de 1983 (Directives), qui attribuent, entre autres, des tâches au Département des finances, soit en particulier à son Secrétariat Général, en sus de celles fixées par la LIPD (article 20). Ces tâches comprennent notamment l'information aux exploitants des fichiers et aux administrés, ainsi que la tenue des registres des exploitants de fichiers (article 20 LIPD et 23 Directives). Cela étant, le Secrétariat Général du Département des finances ne remplit pas les conditions posées par le droit fédéral et communautaire, tant au niveau de son statut que de ses compétences.

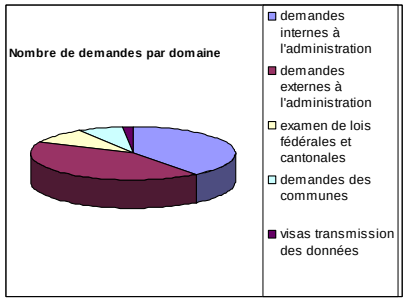
En 2005, le Secrétariat général du Département des finances a consacré environ 200 heures à la protection des données, ce qui correspond environ à 0.15 EPT. Son activité a porté sur le traitement de demandes portant tant sur l'application de la LIPD à des cas pratiques, que sur l'examen de documents sous l'angle de protection des données. Le Secrétariat général est parfois intervenu auprès d'entités soumises à la loi, afin d'améliorer le traitement des données personnelles par les entités soumises à la loi. Enfin, il a eu l'occasion de formuler des observations dans le cadre de consultations de lois, fédérales (par exemple, avant-projet de la révision de la loi sur les documents d'identité de ressortissants suisses – introduction du passeport biométrique -, loi sur l'harmonisation des registres), ou cantonales (avant-projet de loi sur l'aide aux requérants d'asile et à certaines catégories d'étrangers), impliquant le traitement de données personnelles. Il a également participé à des rencontres organisées sur le thème de la protection des données, notamment la 27ème conférence sur la

[23] LIPD, RSV 172.65

protection des données et les préposés à la protection des données, qui s'est tenue le 16 septembre 2005, à Montreux.

Les tableaux ci-dessous permettent d'avoir une vision synthétique de l'activité précitée :





1.3 Structure de l'avant-projet de loi

Disposant de prérogatives en matière de protection des données, le Département des finances, par son Secrétariat général, a été chargé de l'élaboration du présent avant-projet de loi. Cet avant-projet de loi s'inspire non seulement de la loi fédérale sur la protection des données, y compris des dernières modifications, mais aussi de certaines lois cantonales. En effet, le Département des finances a estimé que, eu égard à l'uniformité se dégageant des lois sur la protection des données en Suisse, il était opportun de s'adapter, à tout le moins, à certaines de leurs dispositions.

Au moment de l'élaboration du présent avant-projet de loi, le Département des finances a examiné l'opportunité de suivre l'exemple fourni par certains cantons, qui ont choisi de traiter la question de la transparence de l'administration et la protection des données cantonale dans une seule et même loi. Il y a renoncé pour les raisons suivantes. Tout d'abord, le fait de remplacer une loi récente (la loi sur l'information – LInfo - est entrée en vigueur le 1er septembre 2003) ne se révélait pas souhaitable, dans la mesure notamment où les entités qui y sont soumises ne s'y sont conformées que récemment son application n'a pas encore pu faire l'objet d'une évaluation approfondie (en effet, un seul rapport du 21 février 2005). Deuxièmement, le fait de soumettre la transparence de l'administration et la protection des données à deux lois distinctes n'empêche nullement une harmonisation des dispositions qui leur sont en tout ou partie communes (par exemple, entités soumises à la loi, conditions dans lesquelles

des données peuvent être obtenues, droit des personnes concernées). A ce titre, il convient de relever que les lois ou projets de lois cantonales traitant des deux sujets disposent d'un chapitre dédié à la protection des données, et d'un chapitre consacré à la transparence : seules quelques dispositions sont communes. Enfin, les cantons qui connaissent une seule loi régissant les deux sujets précités attribuent à un seul organe, ou préposé, les missions de surveiller l'application de la loi ; c'est également le cas de la LTrans et de la LPD. Cette solution a été retenue en tenant compte du fait que la procédure d'accès à des documents officiels peut poser des questions ayant trait à la protection des données. Elle permet aussi de ne pas affaiblir la protection des données par l'introduction du principe de la transparence, et d'assurer une unité de doctrine dans le respect de ces deux grands principes, qui impliquent tous deux une pesée des intérêts en présence : d'un côté, le droit à l'information et à accéder à des documents officiels, et de l'autre le droit de voir sa personnalité protégée. Le fait d'attribuer ces deux domaines à une seule entité permet également de gagner du temps et d'éviter que certaines questions ne puissent être traitées en raison du fait qu'elles soulèvent soit des problèmes en matière de transparence, soit en matière de protection des données. Le Conseil d'Etat a dès lors décidé de ne procéder qu'à une légère adaptation de la LInfo, et d'élaborer une loi distincte pour la protection des données. Le présent avant-projet de loi propose de confier au futur Préposé la tâche de veiller à l'application des deux lois.

Un premier avant-projet a fait l’objet d’une pré-consultation auprès d’entités et de personnes compétentes en matière de protection des données, ou ayant quotidiennement à traiter de données personnelles, soit : les Préposés de Soleure et de Bâle-Campagne, le Département de la formation et de la jeunesse, la Chancellerie, le Service juridique et législatif, le Service des assurances sociales et de l'hébergement, la Police cantonale, le Service cantonal de recherche et d'information statistiques, le Service de prévoyance et d'aide sociales, les Hospices, l'Office de la sécurité informatique cantonale ainsi que la Direction, Planification et Stratégie Informatique. Leurs remarques ont été dans une très large mesure intégrées dans l'avant-projet de loi proposé.

2. OBJECTIFS DE LA LOI

Le présent avant-projet de loi a pour but de fournir un cadre juridique adéquat au traitement des données personnelles dans le secteur public, que ce soit par les autorités cantonales ou communales, par les collectivités et établissements de droit public ou par les personnes privées auxquelles des tâches d’intérêt public sont confiées.

2.1 Définitions

La LIPD ne contient aucune définition ; celles-ci ne se trouvent que de manière éparse dans la loi ou les Directives. Par souci de clarté, une liste de définitions figure désormais dans la loi, à l'instar de ce qui se fait dans la LPD (article 3), et dans d'autres lois cantonales. De surcroît ces définitions sont en grande partie adaptées à celles de la Directive 95/46/CE (article 2).

2.2 Principes

Le traitement des données personnelles doit se faire dans le respect de la vie privée et familiale des personnes, et seules les données nécessaires à l'accomplissement des tâches des autorités peuvent être traitées. Par conséquent, les entités soumises à la loi sont tenues de traiter les données personnelles selon certains principes.

Bien que la LIPD repose sur trois principes, soit celui de la *transparence*, celui de la *proportionnalité* et celui de la *spécialité*, ces derniers ne figurent pas en tant que tels dans la loi. Par contre, d'autres règles applicables au traitement des données, contenues dans la LIPD, sont érigées en principes dans certaines loi sur la protection des données : tel est le cas par exemple de l'exactitude des données (article 4 LIPD) et de la sécurité (article 6 LIDP).

Les principes applicables au traitement des données sont désormais ancrés dans la loi. Ils constituent le noyau dur de la protection des données; il s'agit de la légalité, la finalité, la proportionnalité, la transparence, l'exactitude, la sécurité et la conservation. Ils correspondent à ceux posés par le droit communautaire de même que, dans une large mesure, par la LPD, à son article 4, récemment modifié, en ce sens où le caractère reconnaissable de la collecte pour la personne concernée doit être désormais assuré.

2.3 Devoir d'informer

Le devoir d'informer repose sur le principe de la transparence. Si la loi actuelle reconnaît aux personnes concernées un large droit d'accès (article 7 LIPD), le présent avant-projet de loi va plus loin puisqu'il impose au responsable du traitement de leur fournir des renseignements lors de la collecte des données. Ce devoir incombe aux entités collectant les données, qui doivent fournir aux personnes concernées certaines informations importantes en matière de traitement de leurs données personnelles. Le devoir d'informer est conforme au droit communautaire (notamment article 10 de la Directive 95/46/CE). Dans le cadre de l'actuelle révision de la LPD, ce devoir a toutefois été réduit aux seules données sensibles, le groupe de travail ayant participé à l'élaboration de la loi étant d'avis que, s'il s'étendait à toutes les données, cela aurait constitué une

contrainte excessive pour les maîtres des fichiers[24]. Contrairement à la modification précitée, le présent avant-projet de loi ne restreint pas ce devoir aux seules données sensibles.

2.4 Communication

La communication des données constitue l'une des opérations entraînant le plus de risques pour les personnes concernées. Le régime prévu par la LIPD distingue entre la transmission des données en général, et celle faite au sein de l'administration cantonale. En principe, la transmission ne peut avoir lieu que si une disposition légale le prévoit ; à défaut d'une telle disposition, elle nécessite une décision de l'exploitant, qui doit être inscrite dans le registre des transmissions (article 5 alinéa 1 et 4 LIPD). Pour l'administration cantonale, le Conseil d'Etat est seul compétent pour autoriser une transmission de données personnelles à des tiers extérieurs à l'administration, en l'absence d'une disposition légale. Il est aussi compétent pour autoriser l'accès direct à un fichier, et ceci pour les bénéficiaires à l'intérieur, comme à l'extérieur de l'administration cantonale (article 12 LIPD). Les décisions prises par le Conseil d'Etat en vertu de cette disposition sont toutefois rares, soit moins de cinq par année.

Les règles applicables à la transmission des données ne sauraient toutefois entraver une saine collaboration des entités soumises à la présente loi, afin notamment de ne pas assaillir les personnes de demandes relatives à la collecte de mêmes données. Par conséquent, un juste équilibre doit être trouvé entre, d'une part, la limitation de la communication des données personnelles aux fins d'éviter les atteintes des personnes concernées et, d'autre part, l'échange de données entre les entités soumises à la présente loi.

Une disposition particulière concerne le flux transfrontières des données. Pour qu'une communication puisse se faire, il faut que la législation de l'Etat destinataire assure un niveau de protection adéquat. Ce niveau est adéquat lorsque la législation répond aux exigences posées par le Protocole additionnel. Le Préposé fédéral tient une liste des Etats qui remplissent ces conditions.

2.5 Traitement de données par un tiers

Lorsqu'une entité soumise à la loi confie à un tiers le traitement de données, ce dernier doit se conformer aux principes et règles posés par l'avant-projet de loi. La LIPD autorise déjà, implicitement, la sous-traitance de données à un tiers, puisque son champ d'application s'étend également aux fichiers informatiques

[24] FF 2003, p. 1937

exploités par l'intermédiaire de tiers (article 2 al. 2 LIPD). Le présent avant-projet de loi apporte toutefois des précisions en la matière.

2.6 Registre des fichiers

Le registre des fichiers constitue l'un des éléments clés du droit d'accès, duquel découlent les droits des personnes concernées (rectification, suppression, etc.). Il permet également à l'administration d'avoir une vue d'ensemble sur les fichiers traités par ses services. Un tel registre n'existe pas encore ; seuls des formulaires intitulés « descriptifs des fichiers », conservés sous forme papier au Secrétariat général du Département des finances, permettent de connaître les fichiers existants, leur contenu et leur exploitant. La constitution d'un tel registre permettra aux différents services de mettre à jour, si besoin, les informations contenues à l'heure actuelle dans les descriptifs des fichiers précités. Afin d'assurer une visibilité optimale à ce nouveau registre, l'avant-projet de loi prévoit que le registre sera mis en ligne, à l'instar de ce qui se fait pour les documents officiels de l'administration, en application de la loi sur l'information (article 8 de la loi sur l'information).

2.7 Vidéosurveillance

Le climat d'insécurité grandissant, ainsi que la montée du terrorisme, ont favorisé le développement de moyens de surveillance de plus en plus élaborés, parmi lesquels la vidéosurveillance. Le recours à des caméras de surveillance se généralise, au mépris parfois du respect des droits fondamentaux des personnes qui y sont soumis.

On distingue habituellement entre la vidéo tendant à surveiller des mouvements dans un endroit donné (appelé parfois vidéosurveillance *d'observation*, ou *Verkehrsüberwachung*[25]), qui ne vise pas le traitement de données personnelles, la *vidéosurveillance invasive*, qui tend à surveiller une personne en particulier, à son insu, dans le cadre par exemple d'une enquête de police, et la *vidéosurveillance dissuasive*, à laquelle on recourt pour éviter la perpétration d'infractions sur un certain lieu. Compte tenu des atteintes différentes qu'elles portent aux droits des personnes surveillées, ces différents types de surveillance ne sont pas soumis aux mêmes règles. La vidéosurveillance invasive ne peut être ordonnée que dans le cadre d'une procédure pénale ou par la police ; elle doit par conséquent respecter les règles applicables en la matière. La vidéosurveillance d'observation n'implique pas le traitement de données

[25] Markus Müller / Ursula Wyssmann, "*Rechtssetzungszuständigkeit der Stadt Bern im Bereich der Videoüberwachung*", août 2005, p. 4

personnelles. Par conséquent, l'installation de caméras de surveillance, telle que visée par la motion, concerne la vidéosurveillance dissuasive. Certains procèdent à d'autres distinctions, selon par exemple que les images sont enregistrées ou non, sur un support permettant de zoomer ou non sur une personne en particulier, etc.

La vidéosurveillance visée par le présent avant-projet de loi concerne exclusivement le domaine public cantonal et communal. En effet, le droit suisse distingue entre le traitement des données par les autorités fédérales et les privés, qui est soumis à la LPD, et celui effectué par les cantons et communes, qui est régi par les dispositions légales cantonales et communales. Par conséquent, la vidéosurveillance mise en place par les autorités cantonales et communales ne peut s'exercer que sur le *domaine public*, qui recouvre l'ensemble des choses et des biens qui peuvent être utilisés par tout un chacun, et sur le *domaine administratif*, formé par les biens immobiliers des collectivités publiques qui sont affectés à la réalisation d'un intérêt spécial (écoles, gares, hôpitaux, etc.).

Cette précision apportée, il convient d'examiner les exigences posées pour l'installation de vidéosurveillance dissuasive.

Conformément au principe de la légalité, repris à l'article 4 de l'avant-projet de loi, toute activité étatique doit reposer sur une base légale. A l'heure actuelle, seul le canton de Bâle-Ville a adopté une disposition sur la vidéosurveillance dans les lieux ouverts au public dans sa loi sur la protection des données. D'autres cantons s'apprêtent à le faire, notamment suite au dépôt d'initiatives parlementaires[26]. Certaines communes ont adopté un règlement sur l'installation de caméras de surveillance[27]. La LPD ne contient aucunes dispositions y relatives ; seules certaines ordonnances du Conseil fédéral prévoient l'installation de vidéosurveillance[28]. Certains cantons ont encore édicté des aides-mémoires ou des directives concernant l'installation de vidéosurveillance[29].

---

[26] Tel est notamment le cas de Berne, d'Argovie, de Berne. Le Conseil d'Etat du Canton de Genève a déposé, le 7 juin 2006, un projet de loi sur la protection des données personnelles (PL 9870), qui contient un article 12 sur la vidéosurveillance.

[27] C'est le cas de la Commune de Marly (Fribourg), qui a édicté une disposition spécifique à la vidéosurveillance dans son règlement de police du 18 mars 1987 ; article 20 bis)

[28] Ordonnance réglant la surveillance de la frontières verte au moyens d'appareils vidéo, RS 631.09; Ordonnance sur la vidéosurveillance des Chemins de fers fédéraux, RS 742.147.2.; Ordonnance sur les maisons de jeu, RS 935.521.

[29] Tel est le cas des cantons de Fribourg ("*Aide-mémoire concernant la surveillance vidéo effectuée par des organes publics cantonaux et communaux dans les lieux et bâtiments publics*", consultable sur le site www.fr.ch/sprd) et de Lucerne (*Merkblatt zur Videoüberwachung durch Gemeinden und*

S'agissant de la compétence d'édicter des dispositions légales régissant la vidéosurveillance en matière cantonale, elles varient selon les régimes applicables à la surveillance du domaine public concerné. En ce qui concerne les communes vaudoises, elles disposent d'autonomie dans le domaine de la gestion du domaine public (article 139 alinéa 1 lettre a Cst-VD). La loi sur les communes (LC, RSV 175.11) inscrit l'administration du domaine public, le service de la voirie et, dans les limites de la loi spéciale, la police de la circulation parmi les tâches des autorités communales (article 2 LC). S'agissant des attributions de la municipalité, elles s'étendent notamment à l'administration du domaine public et des biens affectés aux services publics (article 41 al. 1 chiffre 2 LC). La question de savoir si la vidéosurveillance dissuasive s'inscrit dans la gestion ou l'administration du domaine public peut se poser. Cela étant, afin d'assurer des règles uniformes applicables à l'installation de caméras de surveillance, le Conseil d'Etat propose d'inscrire, dans l'avant-projet de loi sur la protection des données, des dispositions y relatives, qui s'imposeront à l'ensemble des autorités publiques soumises à la loi, y compris communes vaudoises.

Dans la mesure où la vidéosurveillance peut potentiellement porter atteinte aux droits fondamentaux des personnes filmées, elle doit répondre à un certain nombre de conditions découlant du respect des libertés, notamment celle découlant du droit d'être protégé contre l'emploi abusif de données personnelles.

En effet, les données obtenues par les caméras de surveillance sont des données personnelles au sens du présent avant-projet de loi, dès lors qu'elles permettent d'identifier une ou plusieurs personnes (article 3 de l'avant-projet de loi) ; elles doivent en outre être qualifiées de sensibles (article 3 chiffre de l'avant-projet de loi), dans la mesure où il est notamment possible de déterminer l'appartenance des personnes filmées à une religion (comme le port de symboles religieux) ou à une race (couleur de peau).

Par conséquent, les principes posés par l'avant-projet de loi doivent être scrupuleusement respectés dans le cadre de l'installation et de l'utilisation de vidéo de surveillance. Le chapitre consacré à la vidéosurveillance contient un rappel des principes généraux applicables à la protection des données, et institue une procédure particulière, préalable à l'installation de vidéo de surveillance, qui permettra au Préposé de vérifier si les conditions posées par la loi sont respectées. Il devra également examiner si les atteintes aux droits fondamentaux, induites par l'installation de caméras de surveillance, sont justifiées. Pour ce faire, il vérifiera si le but est suffisamment précis dans la base

---

Kanton, disponible sur le site www.datenschutz.lu.ch/index/themen_nav-ilink/videoueberwachung.htm)

légale, si ce moyen de surveillance est propre à atteindre le but visé (soit la non perpétration d'actes pénalement répréhensibles) ou si des meures moins intrusives peuvent être envisagées en lieu et place.

Le Conseil d'Etat apportera des précisions dans un règlement d'application. De cette manière, il sera plus aisé de tenir compte des progrès techniques constatés en matière de vidéo surveillance (notamment développement des "privacy filters", etc.), qui réduisent parfois les atteintes portées à la sphère privée des personnes concernées. L'élaboration de ce règlement se fera, le cas échéant, avec la collaboration du Préposé, qui suivra de près l'évolution de ce domaine au regard des exigences posées par la protection des données.

Le Conseil d'Etat rappelle toutefois que la question de la vidéo surveillance n'est ici traitée que sous l'angle de la protection des données. Ainsi, ni l'opportunité, ni l'efficacité de ce moyen de surveillance, ni les questions de responsabilités des entités ayant recours à la vidéo surveillance, ne sont abordés, ni régis par le présent avant-projet de loi.

Dans le cadre strict posé par le présent avant-projet jet de loi, les autorités compétentes devront décider, à la lumière notamment des principes rappelés aux articles 21 et 22 de l'avant-projet de loi, si l'installation de caméras de surveillance est un moyen adéquat pour la réalisation du but fixé. L'implication du Préposé , dès l'étude du projet, garantira le respect des dispositions légales et règlementaires applicables en la matière.

2.8 Procédure

L'avant-projet de loi institue une procédure souple pour permettre à tout intéressé, dont le demande, fondée sur la loi, n'a pas été accueillie favorablement, de recourir à la médiation de l'autorité chargée de la surveillance des dispositions relatives à la protection des données. Cette dernière dispose pour cela de différents moyens, énumérés pour la loi. Au cas où les parties arrivent à un accord, la procédure est terminée. Sinon, l'autorité émet une recommandation, qu'elle notifie aux parties. Cette recommandation ne doit pas être considérée comme une décision, et n'est dès lors pas sujette à recours au Tribunal administratif. Au cas où l'entité concernée entend ne pas suivre la recommandation émise par l'autorité, elle l'en informe par une décision, qu'elle adresse également à la personne intéressée. Ce n'est que dans cette hypothèse que la procédure devient contentieuse, dans la mesure où l'intéressé peut porter l'affaire devant le Tribunal administratif.

Cette procédure permet ainsi de répondre aux exigences posées par le Protocole additionnel, qui prescrit que l'entité chargée de la surveillance des données doit avoir la faculté de la qualité de recourir contre les décisions prises en matière de

protection des données. Cette compétence est d'ailleurs également reconnue au Préposé fédéral dans le cadre de la révision de la LPD (article 27 alinéa 6 révisé).

2.9 Autorité chargée de la surveillance des dispositions relatives à la protection des données

A l'heure actuelle, la loi vaudoise n'institue aucune autorité chargée de la surveillance des dispositions relatives à la protection des données. Or, selon le Protocole additionnel, chaque Etat partie à la convention doit prévoir une ou plusieurs autorités de contrôle indépendantes (article 1, paragraphes 1 et 3). Ces autorités doivent disposer du pouvoir d'investigation et d'intervention et du pouvoir d'ester en justice ou de porter les violations à la connaissance de l'autorité judiciaire compétente. Chaque autorité de contrôle doit en outre pouvoir être saisie par quiconque invoque la protection de ses droits et libertés fondamentaux à l'égard des traitements de données personnelles qui relèvent de sa compétence (article 1, paragraphe. 2). Les décisions des autorités de contrôle peuvent à leur tour faire l'objet d'un recours juridictionnel (article 1, paragraphe 4). Les autorités de contrôle doivent en outre coopérer entre elles, notamment par l'échange d'informations (article 1, paragraphe 5)[30].

L'indépendance d'une autorité publique se caractérise en général par sa procédure d'élection ou de nomination, par son rattachement à l'un des pouvoirs et par sa marge de manœuvre en matière budgétaire[31].

2.9.1 Nomination

Comme indiqué ci-dessus, les cantons suisses qui ont institué une ou plusieurs autorités chargées de la surveillance des données ont prévu, pour l'élection de ces dernières, des procédures différentes, les uns attribuant cette compétence au Parlement (*Valais*), les autres au Gouvernement (*Neuchâtel*, *Tessin*, *Berne*, *Lucerne*, *Soleure*, *Bâle-Ville*, *Thurgovie*, *Zurich*) ou encore aux deux autorités (*Fribourg*, qui prévoit que le Préposé est élu par le Gouvernement et la Commission, composée de 5 membres, est élue par le Parlement ; *Jura*, où le juriste et l'informaticien composant la commission cantonale de surveillance sont élus par le Parlement, alors que le Gouvernement désigne le troisième membre de la commission, qui la préside).

---

[30] FF 2003, p. 1928

[31] Ces critères ressortent notamment d'une publication établie le 28 octobre 2005 à l'attention des membres de l'association des commissaires suisses à la protection des données, dans le cadre de la transposition des accords de Schengen et de Dublin dans les cantons (en particulier p. 5) (http://www.dsb-cpd.ch/f/publikationen/index.htm)

Ainsi, à deux exceptions près, tous les cantons prévoient que l'autorité chargée de la surveillance est nommée par le Gouvernement.

Pour être indépendante, l'autorité doit pouvoir exercer son activité sans crainte de voir résilier son mandat au cas où elle émet un avis ne convenant pas à son autorité de nomination, soit le gouvernement. La solution consiste à fixer, dans la loi, la durée du mandat de l'autorité et de prévoir qu'une résiliation avant l'échéance du terme fixé par la loi ne puisse se faire que de manière exceptionnelle. La durée de ce mandat est fixée à 5 ans, durée qui correspond à celle de la législature. L'autorité peut être reconduite dans sa fonction, pour la même durée, ceci sans limitation de nombre de mandats.

2.9.2 Rattachement

Pour exercer ses tâches d'une manière indépendante, l'autorité ne doit pas avoir de lien de subordination direct avec une autre entité qu'elle pourrait être amenée à contrôler. Les systèmes institués dans les autres cantons sont assez divers. Certains ne prévoient aucun rattachement de l'autorité de surveillance : il s'agit en général des cantons ayant institué des commissions de protection des données (*Neuchâtel, Jura*). Dans d'autres cantons, l'autorité est rattachée à la Chancellerie (*Soleure, Bâle-Ville*) ; dans ce cas, l'autonomie et l'indépendance de l'autorité sont garanties. D'autres cantons prévoient enfin un rattachement au Département de justice et police (*Lucerne*) ou au Département de justice, affaires communales et ecclésiastiques (*Berne*). Quant au Préposé fédéral, il est rattaché à la Chancellerie fédérale.

Le Canton de Vaud connaît déjà des autorités qui, bien qu'exerçant ses missions légales de manière indépendante, sont administrativement rattachées à un département : le Bureau de médiation administrative, rattaché à la Chancellerie, elle-même rattachée administrativement au département précité, l'Autorité de surveillance des fondations, ainsi que le Contrôle cantonal des finances, rattachés au Département des finances. Lors des récents débats, l'indépendance du Contrôle cantonal des finances, nonobstant son rattachement, a été confirmée. Aussi le présent avant-projet de loi propose-t-il de rattacher l'autorité chargée de la surveillance de la protection des données à la Chancellerie. Ce rattachement suit une certaine logique puisqu'il vient compléter un dispositif tendant à assurer la transparence de l'activité de l'administration, mis en place avec la loi sur l'information, qui attribue notamment à la Chancellerie le Bureau d'information et de communication (article 4 du règlement d'application de la loi sur l'information)[32]. C'est en outre à la Chancellerie qu'il revient d'établir la

[32] RSV 170.21.1

liste des documents officiels conformément à la loi (article 37 du règlement d'application de la loi sur l'information).

Il convient de noter à ce titre que certains cantons ont procédé à une fusion des domaines de l'information et de la protection des données, en adoptant une loi commune aux deux domaines (voir par exemple la loi sur l'information et la protection des données du 21 février 2001 du canton de *Soleure*; les cantons de *Neuchâtel* et de *Zurich* ont également élaboré des projets de loi analogues).

2.9.3 Moyens financiers

L'autorité chargée de la surveillance des données doit disposer des moyens nécessaires à l'accomplissement de ses tâches, qui sont énumérées dans le présent avant-projet. Certaines d'entre elles vont générer de nouvelles dépenses, en particulier en matière de publication et de maintenance du site Internet. Le budget de l'autorité sera intégré à celui du Département auquel elle est rattachée.

2.9.4 Structure de l'autorité

La surveillance des données est confiée, suivant les cantons, à un ou plusieurs Préposés ou Délégués (*Lucerne, Soleure, Thurgovie, Bâle-campagne, Zurich*), à une commission (*Jura, Neuchâtel, Bâle-Ville*), ou aux deux (*Tessin*, *Fribourg*).

En raison de l'indépendance inhérente à la fonction, la personne chargée de la surveillance des données ne peut exercer d'activité accessoire ou, à tout le moins, d'activité accessoire susceptible d'entraver son indépendance. Or, eu égard à la charge de travail actuelle (cf. au chapitre 1.2.3 ci-dessus), il est difficile, du moins à l'heure actuelle, d'envisager une commission composée de plusieurs membres qui se consacreraient exclusivement à la surveillance des données. Cela conduit dès lors à privilégier la nomination d'un-e Préposé-e. En outre, un poste à temps partiel doit être envisagé.

2.9.5 Préposé à la protection des données et à l'information

Comme indiqué ci-dessus, le présent avant-projet de loi institue un seul Préposé qui aura pour tâche de surveiller l'application de la présente loi, ainsi que de la LInfo.

Le sort de la commission restreinte, prévue à l'article 21 de la LInfo, doit par conséquent être réglé. Cette commission peut être saisie par l'intéressé dont la demande de transmission d'information a été refusée, restreinte ou différée assure la médiation, afin d'assurer la médiation entre lui et l'entité concernée (article 21 LInfo). La commission délivre une recommandation écrite au cas où la médiation échoue ; elle ne peut cependant pas rendre de décision. Depuis sa

mise en place, la commission restreinte n'a été saisie que quelques fois par les administrés, quand bien même sa médiation aurait pu conduire à une solution satisfaisante pour les parties. La modification proposée par le Conseil d'Etat prévoit que la commission restreinte prévue par la LInfo soit remplacée par le Préposé à la protection des données et à l'information, qui assurera les mêmes prérogatives, à la différence près que sa médiation n'est plus facultative mais obligatoire ; aussi la faculté de choisir entre la commission ou le Tribunal administratif est-elle supprimée. Cela favorisera la médiation préalable à la saisine de l'autorité judiciaire. La solution consistant à instituer un Préposé chargé de la protection des données et de la transparence s'apparente à celle retenue par le droit fédéral, qui prévoit que le Préposé fédéral à la protection des données et à la transparence assure un rôle de médiateur, sans pouvoir rendre de décision (articles 13 et suivants LTrans).

2.9.6 Tâches

La première tâche du Préposé est d'assurer la surveillance du respect des dispositions du présent avant-projet de loi. Les autres tâches sont énumérées exhaustivement par la loi. L'avant-projet de loi est sur ce point, ainsi que sur les moyens qui sont à la disposition du Préposé, adapté aux exigences posées en la matière par le droit communautaire. La promotion de la protection des données est également assurée par un rapport public, qui sera établi une fois par année par le Préposé. Ce rapport, qui existe déjà dans la quasi-totalité des cantons suisses, énumèrera les cas traités par le Préposé et fournira un résumé des recommandations qu'il a émises. Le Préposé demeure libre d'y faire figurer les éléments qu'il juge opportuns.

2.9.7 Communes

Le présent avant-projet de loi s'applique également aux communes, qui sont actuellement soumises à la LIPD. Elles disposent toutes d'une commission communale de recours en matière informatique au sens de l'article 17 LIPD, qui connaît des recours exercés contre le refus de transmettre des renseignements, d'admettre l'opposition ou de procéder aux rectifications prévues par la loi. Les décisions de la commission communale de recours peuvent être portées devant le Tribunal administratif. Fort du constat que ces commissions de recours en matière informatique communales n'ont que peu ou jamais siégé depuis leur mise en place, et soucieux d'assurer une cohérence entre le présent avant-projet de loi et la LInfo, le Conseil d'Etat propose de reprendre ce que prévoit cette dernière à son article 26, en indiquant que les autorités communales statuent sur les demandes concernant leurs activités. Les commissions de recours en matière informatique communales n'auront dès lors plus de raison d'être.

3. LOI SUR LA PROTECTION DES DONNEES PERSONNELLES – COMMENTAIRE PAR ARTICLE

3.1 Chapitre premier

Le premier chapitre traite du but et du champ d'application de l'avant-projet de loi, de même que la définition de certaines notions essentielles à la protection des données.

Article 1 – But de la loi

L'article 1 de l'avant-projet de loi reprend les fondements du droit de la protection des données, à savoir la protection de la personnalité. Conformément à l'article 15 alinéa 2 Cst-VD, toute personne doit être protégée contre l'utilisation abusive, par les autorités cantonales ainsi que les autres entités soumises à la loi, des données la concernant. La loi est donc une loi cadre, qui s'applique dès qu'une donnée personnelle est traitée par une des entités énumérées à l'article 2. Elle pose par conséquent des règles minimales en matière de protection des données, qui peuvent être plus restrictives dans des lois spéciales.

Article 2 – Champ d'application

La protection des données personnelles concerne aussi bien les personnes physiques que morales. En ceci, l'avant-projet de loi correspond à la LPD.

L'un des grands changements instauré par le présent avant-projet de loi est l'étendue de son champ d'application à tous les fichiers, qu'ils soient informatiques ou sous forme papier. Cela constitue un changement fondamental par rapport au périmètre de la LIPD, qui ne s'étend qu'aux fichiers informatiques ou aux fichiers manuels exploités en liaison avec une installation de traitement automatisé de données.

La loi s'applique à tous les services de l'Etat, aux communes ainsi qu'aux corporations et établissements de droit public. Les personnes privées qui se voient confier des tâches publiques par le canton ou les communes sont également soumises à la loi. Il n'y a dès lors pas de changement par rapport à la loi actuelle. Toutes les personnes morales ou physiques (c'est-à-dire les établissements et les corporations de droit public), auxquelles l'Etat ou les communes confient des tâches publiques, sont visés ; aucune liste particulière ne doit par conséquent être établie, contrairement à ce qui est prévu par la LInfo (article 2 alinéa 2 et article 3 du règlement d'application). Le champ d'application de l'avant-projet de loi est donc plus large que celui de la LInfo. En effet, certaines entités, comme les Eglises ou les Retraites populaires,

exclues du champ d'application de la LInfo, sont soumises au présent avant-projet de loi lorsqu'elles exercent des tâches publiques. Pour ce motif seulement, il n'est pas possible de calquer le champ d'application à raison des personnes du présent avant-projet de loi à celui de la LInfo.

L'alinéa 3 soustrait du champ d'application les délibérations du Grand Conseil (au sens large, à savoir au plénum et aux commissions du Grand Conseil) et des conseils généraux et communaux, qui sont régies par des règles particulières, contenues dans la loi sur le Grand Conseil[33] (articles 162 à 168) et la loi sur les communes[34] (article 27). Sont également soustraites au champ d'application de la loi les procédures pendantes civiles, pénales et administratives. En effet, des règles spécifiques s'appliquent déjà à ces procédures, notamment en vue de protéger la personnalité des personnes impliquées, comme le droit d'être entendu, le droit d'accéder à son dossier, le droit de participer à l'administration des preuves, les règles applicables à la déposition en justice. Seule la procédure administrative de première instance, soit la procédure administrative non juridictionnelle, est soumise à la loi. Ces deux exceptions correspondent à ce qui est prévu par la LPD (article 2 lit. b et c). Les personnes physiques ou morales, visées à l'article 2 alinéa 1 lit. c), ne sont pas soumises à la loi lorsqu'elles accomplissent des activités relevant du droit privé. Dans ce cas là, la LPD est applicable. Enfin, les outils de travail, hautement personnel, des entités soumises à la loi, ne sont pas non plus soumis à cette dernière.

La LIPD exclut actuellement de son champ d'application la loi sur les dossiers de police judiciaire, qui sont régis par une loi spécifique[35]. Dans la mesure où le présent avant-projet de loi est une loi cadre, l'exclusion de la loi sur les dossiers de police judiciaire ne se justifie plus ; en revanche, cette dernière pose des règles spécifiques en la matière, qui peuvent déroger, le cas échéant, préciser les dispositions du présent avant-projet de loi.

En ce qui concerne la Banque Cantonale Vaudoise, qui est exclue du champ d'application de la LIPD (article 2 alinéa 3), elle n'est pas soumise à l'avant-projet de loi. En effet, dans la mesure où elle déploie ses activités principalement dans le domaine privé, elle doit être soumise à la LPD, et non au présent avant-projet de loi.

---

[33] RSV 171.01
[34] RSV 175.11
[35] Loi du 1er décembre 1980 sur les dossiers de la police judiciaire, RSV 133.17

Article 3 – Définitions

Les définitions des termes habituellement utilisés en matière de protection des données[36] figurent désormais dans la loi, à l'instar de ce qui est prévu dans les autres lois fédérale et cantonales de la protection des données.

1) données personnelles

Il s'agit de toute information concernant une personne physique identifiée ou identifiable. La personne est identifiée lorsqu'il ressort de renseignements qu'il s'agit de cette personne et d'elle seule ; cela peut être, par exemple, une pièce d'identité. Ces données peuvent prendre la forme de mots, d'images, de signes ou de caractéristiques biométriques (par exemple, empreinte digitale, iris, etc). Par identifiable, on entend une personne qui peut être identifiée, directement ou indirectement, par référence par exemple à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Cela étant, lorsque les moyens nécessaires à l'identification d'une personne sont tels qu'il est peu probable que quelqu'un les mette en œuvre, il n'est plus possible de parler d'identification. Il en est de même lorsque les données sont rendues anonymes. Il n'est pas toujours facile de distinguer entre la nature « identifiable » ou « anonyme » d'une donnée, en raison notamment des moyens offerts par la technique de procéder à une recherche. Aussi faudra-t-il apprécier, de cas en cas, si l'on est en présence d'une personne identifiable ou non.

2) données sensibles

La distinction entre, d'une part, données personnelles et, d'autre part, données sensibles se justifie par le fait que l'atteinte à la personnalité est accrue lorsque les données ont trait à certains aspects de la vie privée d'une personne. La loi actuelle ne contient pas une telle distinction, contrairement à la plupart des lois cantonales, à la loi fédérale et au droit communautaire (par exemple, article 3 lit. e LPD et article 6 de la Convention STE n° 108, qui les nomme « catégories particulières de données »). Le traitement de ces données doit répondre à des exigences particulières, qui sont énumérées dans la loi (cf. articles 4 alinéa 2 et 14 alinéa 2, 2ème phrase).

Ces données sont les suivantes :

(i) les opinions ou activités religieuses, philosophiques, politiques ou syndicales

(ii) la santé, la sphère intime ou l'appartenance à une race : la santé recouvre toute information médicale, qui peut donner une image négative de la personne

[36] Voir message du CF, relatif à la LPD, ad. article 3

concernée. La sphère intime comprend toutes les données qu'une personne ne divulgue qu'à ses proches, en raison de leur grande connotation affective.

(iii) les mesures d'aides sociales ou d'assistance : ces mesures sont en effet intimement liées à la vie privé de la personne concernée. Elles se rapportent aux prestations des assurances sociales en rapport avec la maladie ou l'accident, de même que la tutelle ou l'aide sociale. Il s'agit, par exemple, des prestations complémentaires, les indemnités chômage, des prestations versées aux personnes handicapées ;

(iv) les poursuites ou sanctions pénales et administratives :

3) profil de la personnalité

Le profil de la personnalité est un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. Cette notion set parfois vague et il conviendra de déterminer, de cas en cas, si les données traitées permettent d'obtenir le profil de la personnalité d'un individu ou non. Selon la Commission fédérale de la protection des données (JAAC 65.48), la durée constitue un élément important, dans la mesure où une collecte de données personnelles, étalée sur plusieurs années, permet d'obtenir un profil de la personnalité.

4) personnes concernées

La personne concernée est celle dont les données sont traitées. Il s'agit indifféremment de personnes physiques ou morales, de droit privé ou de droit public.

5) traitement de données personnelles

Le terme de « traitement » est très large, les opérations énumérées dans la loi n'étant pas exhaustives. Le champ d'application prévu est dès lors plus large que celui de la LIPD, cette dernière ne s'appliquant qu'au traitement des fichiers informatiques. Cette disposition est pour le surplus adaptée à ce qui est prévu dans la Directive 95/46/CE (article 2 lit. b).

6) communication

Bien que la communication soit une forme de traitement, elle doit faire l'objet de règles particulières en raison des graves atteintes qu'elle représente.

7) fichier

Est fichier tout ensemble de données qui se rapporte à plus d'une personne. Ce qui importe, c'est la possibilité de rechercher une personne concernée dans un ensemble de données, et ce quelle que soit la structure et l'organisation du fichier. L'accès à ces données doit cependant être possible sans mettre en œuvre

des moyens disproportionnés. L'avant-projet de loi ne fait dès lors plus de distinction entre fichier informatique et fichier manuel, contrairement à la LIPD, qui ne s'appliquait qu'aux fichiers informatiques ou aux fichiers manuels, exploités en liaison avec une installation de traitement automatisé des données. En cela, l'avant-projet de loi se conforme à ce qui est prévu tant par la Confédération que par les cantons. La notion de fichier ne s'étend toutefois pas aux outils de travail des collaboratrices et collaborateurs des entités soumises à la présente loi, comme par exemple les agendas ou autres listes d'adresses.

8) responsable du traitement

C'est la personne en charge du traitement des données personnelles. Ce terme correspond à celui utilisé dans le droit communautaire (article 2 lit. d de la Directive 95/46/CE) ; les autres cantons utilisent en majorité le terme de « maître du fichier ». Le responsable du traitement décide le contenu et la finalité du fichier, soit, en d'autres termes, son but. Il correspond à "l'exploitant du fichier", tel qu'institué par la LIPD. Au sein de l'administration cantonale, le responsable du traitement est le service qui exploite le fichier concerné. S'agissant d'une unité plus petite (par exemple, office, école, etc.), elle doit également être considérée comme le responsable du traitement. A l'heure actuelle, le secrétariat général de chaque département, ainsi que celui de l'ordre judiciaire, doit établir la liste des exploitants du fichier (article 5 alinéa 3 des Directives) ; le règlement du présent avant-projet de loi pourra prévoir une obligation analogue. La notion de responsable du traitement est importante, car elle entraîne des obligations de la part de l'entité considérée comme telle. Aussi cette dernière ne peut-elle se soustraire à ses responsabilités en invoquant, par exemple, que la gestion du fichier relève d'informaticiens.

9) sous-traitant

Le sous-traitant est celui qui traite, pour le compte du responsable du traitement, les données personnelles. Cela peut être des personnes physiques, comme des personnes morales.

10) *consentement de la personne concernée*

La personne concernée est toujours libre de fournir, de son propre chef, les données personnelles la concernant, alors même qu'aucune disposition légale ne le prévoit. Ce consentement doit toutefois être donné de manière éclairé, et non sous la contrainte, et la personne doit connaître l'utilisation qui sera faite de ses données personnelles.

11) procédure d'appel

La procédure d'appel est un mode de communication des données permettant à un tiers de consulter lui-même un fichier, moyennant un accès direct à ce

dernier, par exemple par l'octroi d'un mot de passe (principe de *self-service*). Cette communication doit faire l'objet de règles précises et dans le respect des dispositions légales applicables au domaine concerné, dans la mesure où elle dépend de la seule volonté du tiers, dès que ce dernier dispose de l'accès au fichier, et échappe dès lors au contrôle du responsable du fichier. La procédure d'appel peut concerner des fichiers tenus par des services de l'Etat, mais également des fichiers de la Confédération.

12) destinataire

La notion de destinataire correspond à celle de tiers de la LIPD (article 5). Elle vise tout bénéficiaire d'une transmission de données, qu'il soit à l'intérieur ou à l'extérieur de l'administration cantonale pour les organes cantonaux, ou externe aux autres entités soumises à la présente loi. Cette définition est adaptée à celle de l'article 2 lit. h de la Directive 95/46/CE.

13) Entités

Ce sont les entités qui sont soumises à la loi (article 2).

14) loi au sens formel

Par loi au sens formel, on entend les décrets et lois adoptés par le Grand Conseil; au niveau communal, il s'agit des règlements adoptés par le conseil général ou communal. La distinction est importante dans la mesure où le traitement de certaines données, nécessitant un degré particulier de protection (article 4 alinéa 2), ainsi que certaines communications, échappant au contrôle du responsable du traitement (article 14 alinéa 2), requièrent une loi au sens formel.

3.2 Chapitre II Dispositions générales

Ce chapitre contient les principes applicables en matière de protection des données. Ces principes sont le fondement même de tout traitement de données personnelles. Il s'agit des principes de la légalité, la finalité, la proportionnalité, la transparence, l'exactitude, la sécurité et la conservation. Deux de ces principes sont déjà reconnus actuellement par la LIPD : celui de la transparence et de la proportionnalité. Le troisième, soit celui de la spécialité, n'est pas repris. Contrairement au droit fédéral, où ces principes sont énumérés dans un seul article (article 4), l'avant-projet de loi consacre un article par principe.

Article 4 – Légalité

Comme toute activité de l'Etat, le traitement des données personnelles doit avoir un fondement dans la loi. Ce traitement, y compris la création de fichier, doit être en général expressément prévu dans des lois. Il peut également arriver

que, sans reposer sur une base légale, le traitement s'effectue par une autorité dans l'accomplissement de sa tâche qui est, elle, prévue dans la loi. Il convient dès lors de regarder, dans un premier temps, si la base légale prévoit le traitement de données personnelles ; ce dernier ne pourra alors se faire que dans le but fixé par la loi. Si seule la tâche légale est prévue, un examen, de cas en cas, devra être effectué pour savoir si l'exécution de la tâche, telle que fixée dans la loi, comprend le traitement des données envisagé.

Lorsque les données traitées sont des données sensibles, le principe de la légalité est renforcé et d'autres conditions sont posées : le traitement doit être prévu par une loi au sens formel (ce terme est défini à l'article 4 alinéa 2 de l'avant-projet de loi), l'accomplissement d'une tâche doit être clairement défini dans une loi au sens formel, ou la personne concernée a elle-même fourni ces données à tout un chacun, ou y a consenti. Ce consentement doit être donné de manière consciente par la personne concernée, et ne peut être déduit du seul fait de mettre des données personnelles à disposition, par exemple sur des sites Internet (*blogs*, etc.) ou des "*chats*". Ces conditions sont alternatives et non cumulatives.

Article 5 – Finalité

Il est important que les données soient traitées à des fins spécifiques ; ces fins peuvent être signalées soit lors de leur collecte, soit découler d'une loi, soit ressortir des circonstances. Le principe de la finalité découle, d'une certaine façon, du principe de la bonne foi, qui régit notamment les activités des autorités. Ainsi, lorsqu'elle fournit ses données personnelles, la personne concernée s'attend à ce qu'elles soient traitées conformément aux fins pour lesquelles elles sont collectées.

Article 6 – Proportionnalité

Selon ce principe, sur lequel repose déjà la LIPD, seules les données nécessaires à l'accomplissement des tâches des responsables du traitement peuvent être traitées. Chacune des entités soumises à la loi devra dès lors examiner de quelles données elle a besoin pour l'accomplissement de ses tâches et procéder à une pesée des intérêts entre l'atteinte potentielle découlant du traitement des données personnelles et les données qui lui sont réellement utiles.

Article 7 – Transparence

Le principe de la transparence est désormais inscrit dans la Constitution cantonale, qui prescrit que l'Etat et les communes informent la population de leurs activités selon le principe de la transparence (article 41 Cst-VD). C'est ce principe qui est également à l'origine de la LInfo, qui a pour but de garantir la

transparence des activités des autorités afin de favoriser la libre formation de l'opinion publique (article 1 LInfo). Enfin, l'actuelle LIPD repose sur ce principe, duquel découle le droit de la personne concernée d'être informée du traitement des données la concernant. Le caractère « reconnaissable » de la collecte des données devra être apprécié de cas en cas, conformément notamment au principe de la proportionnalité. Ainsi, tous les renseignements relatifs à la collecte des données, c'est-à-dire notamment l'identité du responsable du traitement, la finalité du traitement, les éventuels bénéficiaires des données, et tout autre renseignement utile, devront être fournis. Lorsque le consentement est nécessaire (voir par exemple les articles 14 lit. c de avant-projet de loi, soit en cas de communication de données personnelles à des entités soumises au présent avant-projet de loi), ce dernier doit être donné sans équivoque. En effet, dans la mesure où ce consentement constitue un motif justificatif du traitement des données, il est indispensable qu'il soit recueilli par une personne ayant pleinement conscience de sa portée. Ce consentement doit en outre être donné « librement », ce qui exclut tout consentement arraché sous la contrainte.

Article 8 – Exactitude

Tant les personnes concernées que les entités soumises à la présente loi ont intérêt à ce que les données soient exactes, c'est-à-dire qu'elles soient correctes, à jour et complètes. Ce principe implique que les entités veillent à mettre à jour les données, notamment dans le cas où elles envisagent de rendre des décisions concernant les personnes concernées. L'exactitude des données revêtait déjà une grande importance lors de l'élaboration de la LIPD, puisqu'elle la prévoit expressément (article 4), de même que les Directives, qui prescrivent que « les fichiers actifs sont tenus à jour dans la mesure nécessaire à leur utilisation » (article 9).

L'inexactitude des données confère à la personne concernée des droits tendant soit à la correction des données erronées, soit à leur destruction (article 28).

Article 9 – Sécurité

En raison de leur nature, les données personnelles doivent être protégées contre tout danger de destruction, falsification, etc. Sans mesures de sécurité efficace, la protection des données ne peut être assurée. La généralisation de l'informatique, l'envoi de fichiers complexes, la consultation d'Internet, sont autant de dangers potentiels qu'il convient de réduire par tous les moyens possibles. Aussi convient-il de prévoir, comme l'actuelle la LIPD (article 6), que toutes les mesures indispensables à leur sécurité soient entreprises. Ces mesures divergent selon qu'il s'agisse de fichier manuel ou informatique. Pour

ces derniers, elles devront être à la fois techniques (mot de passe, cryptage, anti-virus, utilisation de logiciels protégés, etc.) et organisationnelles. Le règlement du Conseil d'Etat précisera ces mesures, qui sont majoritairement d'ordre technique.

Article 10 – Conservation

Lorsque le responsable du traitement n'a plus besoin des données, il doit soit les rendre anonymes, soit les détruire. Cela permet, d'une part d'éviter que les données traitées deviennent inexactes et, d'autre part, de faciliter le devoir du responsable du traitement en matière de sécurité. La durée de conservation doit être fixée de cas en cas, selon la nature des données et leur utilisation. Par exemple en matière de vidéo surveillance, elle est fixée à 24 heures, sauf exceptions (article 21 alinéa 2 lit. d).

3.3 Chapitre II – Traitement des données personnelles

Ce chapitre s'adresse aux entités soumises à la loi, en leur imposant certaines règles visant, notamment, à permettre aux personnes concernées de faire valoir des droits qui sont les leurs (Chapitre VI). Ces garanties formelles découlent du respect de la personnalité et des droits fondamentaux, notamment de la liberté personnelle.

Article 11 – Devoir d'informer

Le devoir d'information découle du principe de la transparence, inscrit à l'article 7 du présent projet. Il concerne toutes les données et n'est pas restreint aux seules données sensibles, comme le prévoit, par exemple, le nouvel article 7a LPD[37]. En ceci, le présent avant-projet se conforme au droit communautaire[38]. Ce devoir d'information ne doit être respecté que pour autant qu'il n'a pas déjà été donné, soit par le responsable du traitement lui-même, soit par un tiers. La loi ne pose aucune condition de forme ; l'information peut donc être donnée par oral. Cela étant, la forme écrite est privilégiée si l'on veut garder des moyens de preuves. Ce devoir d'informer sera donc respecté s'il apparaît, par exemple, sur un formulaire comportant des données personnelles ; l'essentiel est qu'il soit visible et compréhensible pour la personne concernée.

Les informations qui doivent être fournies à la personne concernée sont énumérées à l'alinéa 2. Il s'agit de l'identité du responsable du traitement, des finalités du traitement, des destinataires et des modalités d'accès aux données,

---

[37] FF 2003, p. 1943

[38] Soit la Directive 95/46/CE, de même que plusieurs autres législations des pays qui entourent la Suisse

ainsi que des conséquences découlant d'un refus de la personne concernée de fournir les données requises. Cette dernière information indique implicitement que la personne concernée a la possibilité de refuser de fournir des données ; ce refus peut cependant avoir des conséquences importantes, qu'il convient de lui exposer clairement. Les informations énumérées ne sont que celles qui doivent être au minimum transmises aux personnes concernées ; elles peuvent bien entendu être plus nombreuses.

Il arrive parfois que ce ne soit pas la personne concernée qui fournit les données, mais un tiers. Dans ce cas, le responsable du traitement doit l'informer au plus tard lors de l'enregistrement de données. La loi pose toutefois des exceptions à cette règle, notamment lorsque l'information requiert des efforts disproportionnés, ou encore lorsque la loi prévoit expressément cette communication. Comme indiqué ci-dessus, la révision de la LPD prévoit un tel devoir d'information, mais seulement pour les données sensibles ; aussi, lorsque les autorités cantonales, dans le cadre de l'exécution du droit fédéral, transmettent de telles données aux autorités fédérales, le devoir d'informer les personnes concernées leur incombera.

Article 12 – Devoir d'informer en cas de décisions individuelles automatisées

Cette disposition découle directement du droit communautaire (article 15 de la Directive 95/46/CE). Il a pour but d'éviter que l'évaluation de la personnalité ne soit effectuée sur la seule base d'une décision automatisée, sans que la personne concernée ne soit informée de la manière dont la décision a été prise. Ce devoir d'information est rempli par une phrase type figurant sur la décision automatisée. Il convient de noter que ce devoir était également prévu dans le cadre de la modification de la LPD (article 7a LPD); cette modification n'a toutefois pas été acceptée par les Chambres fédérales.

Article 13 – Restrictions du devoir d'informer

L'avant-projet de loi restreint le devoir d'informer dans certains cas, énumérés exhaustivement. Il s'agit tout d'abord du cas où une loi au sens formel le prévoit. Des intérêts prépondérants de tiers peuvent également restreindre le devoir d'informer. Le devoir d'information peut enfin être restreint au cas où un intérêt public prépondérant l'oblige, ou lorsque la communication d'une donnée peut compromettre l'instruction d'une cause, pénale ou toute autre procédure d'instruction. Ces restrictions ne sont pas immuables, et le devoir d'information doit à nouveau être respecté lorsque les cas énumérés disparaissent.

Article 14 – Communication

La communication des données constitue l'un des traitements susceptible de porter le plus atteinte à la personne concernée. Les moyens informatiques permettent aujourd'hui de transférer de nombreuses données ou de prévoir des connexions entre elles, rendant ainsi possible la constitution de super fichiers. Cette dérive doit être empêchée, tout en évitant de poser des règles trop restrictives, peu propices à une administration efficace. Il n'est en effet pas souhaitable que les personnes concernées aient à communiquer à de multiples occasions les mêmes données aux différents services de l'administration.

L'avant-projet de loi pose des conditions générales applicables à la communication des données, qui s'appliquent au cas où d'autres dispositions légales spécifiques ne régissent pas ce traitement des données. Les dispositions applicables à la communication des données concernent non seulement la communication entre les services de l'administration cantonale, mais également la communication entre eux et d'autres autorités (communales ou fédérales), de même que la communication avec des personnes privées. Par conséquent, avant de voir si la communication d'une donnée répond aux exigences posées par la loi, il convient de se rapporter aux dispositions légales régissant l'activité du responsable du traitement.

Lorsque les conditions énumérées par l'article 14 sont réunies, le responsable du traitement peut communiquer des données ; la formulation potestative signifie qu'il dispose toujours de la possibilité, s'il estime ne pas devoir donner suite à une demande, de refuser de transmettre les données. Demeurent cependant réservés les cas où il est tenu de communiquer la donnée en vertu d'une disposition légale.

Les conditions posées par la loi sont les suivantes :

- lorsqu'une base légale le prévoit. La base légale en question doit prévoir la communication des données personnelles, et non le traitement de celles-ci de manière générale ;
- lorsque le requérant établit qu'il a besoin des données pour l'accomplissement de sa tâche légale. Là encore, la tâche doit clairement ressortir de la loi sur laquelle le requérant fonde sa demande ;
- en cas d'accord de la personne concernée. L'accord doit spécifiquement porter sur les données dont la communication est requise. Il doit en outre avoir été donné librement ;
- lorsque la personne a elle-même pris l'initiative de porter les données en question à la connaissance de tout un chacun. Cela peut être, par exemple, par la voie de la presse ou par tout autre moyen ;

- enfin, lorsque l'accord de la personne concernée n'est pas donné uniquement pour se soustraire à certaines obligations légales ou contractuelles. On pense ici notamment au droit de la famille, qui pourrait conduire à ce que les coordonnées permettant de localiser le débiteurs de contributions d'entretien puissent être fournies, ou encore à l'employé qui s'oppose au refus de son employeur quant à la transmission de données relatives au paiement des charges sociales. Toutefois, avant de donner suite à la transmission des données, la personne concernée dispose en quelque sorte d'un droit d'être entendu, afin d'exposer les raisons qui le poussent à s'opposer à la transmission des données.

Certaines lois prévoient que certaines données, nécessaires par exemple à identifier et à localiser une personne (nom, prénom, adresse, date de naissance), peuvent être données sur demande, en l'absence même des conditions précitées. Tel est le cas, par exemple, du droit fédéral (article 19 alinéa 2 LPD). Cela étant, ces données, qui ne sont à priori ni sensibles, ni susceptibles de porter atteinte à la personnalité, peuvent, dans certaines circonstances, constituer une grave entrave à la personnalité des personnes concernées. Le cas, par exemple, de Salman Rushdie, qui avait été cité lors de débats parlementaires lors de l'élaboration de la loi fédérale (à cette époque, il faisait l'objet d'un fatwah lancée à la suite de la rédaction de son livre "*les Versets sataniques*"), illustre bien les risques que peuvent encourir certaines personnes en cas de communication de ces données, qui paraissent anodines. Le présent avant-projet de loi ne prévoit donc pas de disposition analogue.

Le deuxième alinéa traite d'un mode particulier de communication, soit la procédure d'appel, également appelée self-service ou liaison en ligne. Cette communication ne peut se faire que si une base légale le prévoit. S'il s'agit de données sensibles, une base légale formelle est nécessaire.

Article 15 – Modalité – forme

Par analogie à ce qui est prévu par la LInfo, la communication des données a lieu sur place, soit à l'endroit où le responsable du traitement exerce son activité. Si le requérant s'en contente, une communication orale est possible.

Article 16 – Modalité – gratuité

Là encore, l'avant-projet de loi reprend ce qui est prévu par la LInfo. Par principe, la communication de données doit être gratuite; elle peut toutefois être soumise au paiement d'un émolument fixé par le Conseil d'Etat.

Article 17 – Communication transfrontières

Comme indiqué ci-dessus, le niveau de protection des données au niveau suisse est plus ou moins le même. Par conséquent, les données communiquées à la Confédération ou aux autres cantons bénéficient d'un niveau de protection identique à celui assuré par le Canton de Vaud en vertu du présent avant-projet de loi. Cela n'est pas le cas pour d'autres pays, vers lesquels les entités soumises à la loi sont parfois amenées à des données. Aussi l'article 17 prévoit-il que les données ne peuvent être transmises qu'aux pays assurant un niveau de protection adéquat des données. Certaines dérogations à ce principe sont énumérées, de manière exhaustive, par l'avant-projet de loi. La communication, par les entités soumises à la loi, de données personnelles à l'étranger n'est pas fréquente à l'heure actuelle ; elle va cependant se développer, notamment dans le cadre de l'application des Accords de Schengen et de Dublin.

Afin de vérifier si le niveau de protection des données des pays destinataires est adéquat, les responsables du traitement se réfèreront à l'avis émis par le Préposé fédéral à la protection des données (article 31 alinéa 1 lit. d LPD).

Cette disposition correspond à l'article 6 révisé de la LPD, qui est adapté aux exigences posées par le droit communautaire en la matière.

Article 18 – Traitement par un tiers

Il arrive que les entités soumises à la loi confient le traitement des données à des tiers. Ainsi l'administration cantonale vaudoise a recours à la société anonyme BEDAG, à Berne, pour le traitement de bon nombre de données.

Le fait de recourir à des tiers ne doit cependant pas se faire au détriment de la protection des données, raison pour laquelle l'avant-projet de loi pose certaines conditions, soit :

- la sous-traitance doit être prévue soit par la loi, soit faire l'objet d'un contrat (il s'agira en général d'un mandat, par lequel le responsable du traitement mandate un tiers pour le traitement des données). Ce contrat doit rappeler tous les principes énoncés dans la loi et définir les règles applicables à la réalisation du traitement des données fournies ;
- pour pouvoir confier à un tiers le traitement des données, le responsable du traitement doit bien entendu être légitimé à traiter lui-même les données ;
- enfin, aucune obligation légale ou contractuelle de garder le secret ne doit empêcher le traitement des données par un tiers.

L'alinéa 2, selon lequel le tiers doit assurer la sécurité des données, poursuit un but didactique en ce sens qu'il rappelle l'un des principes régissant la protection des données ; les autres principes de la loi sont en effet également applicables.

3.4 Chapitre III Fichiers

Comme indiqué ci-dessus, l'administration ne dispose pas d'un registre renfermant l'ensemble des fichiers tenus par les différents responsables de traitement, mais seulement un « descriptif de fichier », remis par les responsables du traitement au Secrétariat général du Département des finances. L'avant-projet de loi comble cette lacune en prévoyant la création d'un registre des fichiers, consultable sur le site Internet de l'administration, qui énumère tous les fichiers tenus par les entités soumises à la loi.

Article 19 – Registre des fichiers

La tenue du registre des fichiers est confiée au Préposé cantonal à la protection des données et à l'information (ci-après : le Préposé). Afin d'assurer une meilleure visibilité, ce registre est consultable sur le site Internet de l'administration cantonale vaudoise ; pour les personnes qui n'auraient pas d'ordinateur, une liste sur papier est également établie. Les règles applicables à la tenue du fichier seront précisées par le Conseil d'Etat ; elles régiront, entre autres, la mise à jour du registre. L'élaboration de ce registre constituera l'une des premières tâches que devra accomplir le Préposé, qui disposera, pour ce faire, du délai transitoire précisé à l'article 46 du présent avant-projet de loi.

Article 20 – Annonce des fichiers

A l'instar de ce qui se fait à l'heure actuelle, les responsables des traitements devront annoncer les fichiers qu'ils constituent. Ce n'est qu'une fois l'aval obtenu de la part du Préposé que le fichier peut être opérationnel. Cette tâche, assumée pour l'instant par le Secrétariat général du Département des finances, vise à assurer que de nouveaux fichiers soient établis en conformité avec la loi sur la protection des données.

Les renseignements à fournir par les responsables du traitement seront fixés par le Conseil d'Etat. Ceci sera fait conjointement avec le Préposé.

3.5 Chapitre IV Vidéo surveillance

Article 21 – Conditions

Comme indiqué ci-dessus, les images filmées par des caméras vidéo constituent des données personnelles. Elles peuvent être qualifiées de sensibles, puisqu'elles permettent en général de connaître, par exemple la religion d'une personne, l'appartenance à une race, ou encore l'éventuelle atteinte à l'intégrité physique (handicap). En outre, lorsqu'elle se sait vidéo surveillée, la personne concernée peut également être amenée à modifier son comportement, ce qui constitue une

atteinte directe à sa liberté de mouvement, qui fait partie intégrante de la liberté personnelle reconnue par la Constitution cantonale (article 12 alinéa 2).

Bien que tous les principes applicables à la protection des données s'appliquent à la vidéo surveillance, l'avant-projet de loi rappelle ceux dont il faut tenir compte tout particulièrement. Ces principes sont les suivants :

- Légalité : la base légale formelle émane de l'autorité compétente en relation avec le domaine public concerné. Les autorités communales devront dès lors édicter un règlement prévoyant l'installation d'un système de vidéo surveillance, ou insérer, dans un règlement existant, une disposition y relative.
- Finalité : lorsqu'on dispose d'images, il peut être parfois tentant de les utiliser pour un autre motif que celui pour lesquelles elles ont été enregistrées. Par conséquent, la finalité doit être précisément fixée dans la base légale, et les autorités compétentes pour le traitement de ces données doivent strictement s'y tenir.
- Proportionnalité : comme indiqué ci-dessus, la vidéo surveillance porte une atteinte particulière aux droits fondamentaux des personnes. Aussi, même s'il est prévu dans une loi ou un règlement, ce moyen ne doit-il être utilisé que s'il apparaît être le plus adéquat pour atteindre le but poursuivi, notamment sous l'angle de la protection des données. Une étude approfondie doit dès lors être effectuée préalablement à la décision d'installer une vidéo surveillance avec le concours du Préposé (art. 40 lit. f). Il faudra en outre utiliser les moyens techniques les mieux à même de protéger la sphère privée des gens (utilisation de filtres d'image, délimitation très stricte des personnes ayant accès à ces images, restriction par rapport au champ vidéo surveillé, etc.).
- Conservation : l'avant-projet de loi pose un délai maximal de 24 heures pour la conservation des données. Si la vidéo surveillance est assurée en ligne (installation de caméra permettant à une équipe de visionner en continu ce qui est filmé), les images devraient être effacées dès que la personne les a visionnées (soit en principe, immédiatement), sauf si elles doivent être conservées à des fins de preuve.

L'implication du Préposé, dès le moment où il est projeté d'installer une vidéo surveillance, assure que les principes applicables soient respectés.

Le Conseil d'Etat peut régler d'autres questions dans un règlement.

Article 22 – Indications

L'article 22 de l'avant-projet de loi poursuit deux buts. Tout d'abord, il vise à ce que les personnes concernées soient conscientes d'être vidéo surveillées, et ce dès le moment où elles entrent dans le champ de vision des appareils de prise d'image. Les indications énumérées à l'article 22 sont impératives ; elles peuvent bien entendu être complétées par d'autres indications.

Deuxièmement, les personnes concernées doivent disposer des indications nécessaires, le cas échéant, à faire valoir leurs droits auprès du responsable du traitement.

3.6 Chapitre V Statistiques, planification et recherche

Article 23 – Statistiques, planification et recherche

Le traitement des données personnelles à des fins statistiques, de planification et de recherche doit bénéficier d'un régime spécial, afin notamment de permettre aux autorités concernées de disposer des données nécessaires à leurs tâches. En échange de cela, toutes les mesures doivent être prises. Cela concerne tout d'abord l'anonymisation des données, qui doit intervenir dès que leur traitement le permet. Des précautions doivent être également prises lors de la communication de ces données. Enfin, seul les résultats ne permettant pas l'identification des personnes concernées peuvent être publiés.

Moyennant le strict respect de ces règles, certaines dérogations à l'avant-projet de loi sont prévues. Tout d'abord, le principe de la légalité ne s'applique pas, ce qui a pour conséquence que des entités chargées d'effectuer des statistiques ou autres recherches peuvent traiter des données sans qu'une disposition légale ne le prévoie; cela comprend également le traitement des données dites sensibles. Ensuite, le principe de la finalité ne trouve pas non plus application, ce qui a pour conséquence que des données récoltées à des fins, par exemple, sociales, médicales, ou autre, peuvent être utilisées pour la réalisation de statistiques ou d'étude. Enfin, les dispositions applicables à la communication des données ne s'appliquent pas non plus.

Ces dispositions régissent les statistiques effectuées par le Service cantonal de recherche et d'information statistiques, ainsi que les autres entités qui ont pour mission de produire des informations statistiques ou des analyses au sens de la loi du 15 septembre 1999 sur la statistique (RSV 431.01).

3.7 VI Droits de la personne concernée

Pour pouvoir être certaines que les données les concernant ne sont pas utilisées de manière abusive, les personnes concernées doivent avoir la possibilité d'entreprendre des démarches auprès du responsable du traitement concerné.

Article 24 – Consultation

Tout un chacun doit avoir la possibilité de consulter les données le concernant. Grâce au registre des fichiers, les personnes peuvent connaître le responsable du traitement des données qu'elles recherchent. La consultation doit non seulement permettre à la personne de connaître les données personnelles traitées à son compte, mais également, le cas échéant, d'avoir la confirmation que ces données n'existent pas (alinéa 2). Afin d'assurer que ce soit la personne concernée, et non un tiers, qui fait usage de son droit de consultation, un document attestant de son identité doit être fourni (alinéa 3).

Certaines dispositions légales contiennent certaines règles spéciales concernant l'accès aux données personnelles, comme par exemple la loi sur la santé publique[39], dont l'article 24 régit le droit d'accès au dossier du patient.

Article 25 – Modalités

La consultation des données se fait sur place, ou par écrit. Par analogie à ce qui est prévu par la loi sur l'information, un émolument peut être perçu.

Article 26 – Restrictions au droit d'accès

Le droit d'accès n'est pas illimité : certaines circonstances peuvent le restreindre, voire l'interdire. Tout d'abord, lorsqu'une loi interdit l'accès aux données personnelles. L'accès peut également être refusé ou restreint au cas où un intérêt public l'exige ; ce sera par exemple le cas où la sécurité de l'Etat s'oppose à la divulgation d'une donnée ou, à tout le moins, commande que cette donnée ne soit transmise qu'ultérieurement. Les intérêts de tiers peuvent également fonder une restriction au droit d'accès. Enfin, il arrive que la protection de la personne elle-même justifie un refus ou une restriction au droit d'accès.

L'alinéa 2 traite spécifiquement du cas des données médicales. L'accès à ces dernières nécessite parfois des explications complémentaires, soit pour des raisons techniques (l'intervention du médecin vise alors à traduire en des termes compréhensibles les données se trouvant dans le dossier médical), ou pour des

[39] RSV 800.01

raisons psychiques (par exemple, lorsque le médecin estime que le patient doit être accompagné lors de la lecture du dossier). Le médecin d'une personne peut en outre estimer qu'il n'est pas opportun de transmettre certaines données au patient. Dans ces cas là, l'avant-projet de loi prévoit que les données médicales sont transmises au médecin. Cela peut être le médecin traitant, ou un autre médecin, que la personne concernée désigne au responsable du traitement.

Article 27 – Droit d'opposition

Le droit d'opposition ne s'applique pas à tout traitement de donnée ; seule la communication des données est visée. Pour pouvoir s'opposer à cette communication, la personne concernée doit faire valoir un intérêt légitime.

Le responsable du traitement peut rejeter l'opposition, ou la lever après un certain temps, lorsqu'une disposition prévoit expressément la communication de la donnée ou lorsque cette communication est indispensable à l'accomplissement de la tâche de l'entité. Plusieurs dispositions légales, cantonales ou fédérales, prévoient expressément la communication des données. Tel est le cas, par exemple, de l'article 21 de la loi sur le contrôle des habitants[40]. Les communes peuvent elles aussi être tenues de communiquer certaines données : c'est le cas, par exemple, des permis de construire délivrés, qui doivent être communiqués à l'Etablissement cantonal de l'assurance incendie (article 18 alinéa 2 de la loi concernant l'assurance des bâtiments et du mobilier contre l'incendie et les éléments naturels)[41].

Article 28 – Autres droits

Les personnes concernées ont également le droit de demander au responsable du traitement de s'abstenir de procéder à un traitement illicite de données, de supprimer les effets d'un traitement illicite de données ou de constater le caractère illicite de leur traitement. Le choix entre la rectification, la destruction ou l'anonymisation des données revient à la personne concernée. En cas de désaccord avec le responsable du traitement, un conseil auprès du Préposé peut être pris. Les conséquences qui pourraient résulter du traitement illicite de données doivent également pouvoir être réparées.

Article 29 – Réponse du responsable du traitement

Si le responsable du traitement ne donne pas suite à la personne concernée, ou n'y donne suite que partiellement, elle doit lui en donner par écrit les raisons.

---

[40] RSV 142.01

[41] RSV 963.41

Sans avoir à être motivée, sa réponse doit contenir les éléments sur lesquels elle fonde son refus. Ces éléments permettent à la personne concernée de déterminer si elle entend saisir le Préposé pour qu'il procède à une médiation.

3.8 Prétention et procédure

Le Chapitre VI concerne la procédure applicable aux demandes fondées sur la loi. La personne concernée, mais également toute autre personne ou entité, qui présente une telle demande doit avoir la possibilité de s'adresser au responsable de traitement, mais également, en cas de divergence avec celui-ci, à une instance indépendante. Ceci est d'ailleurs déjà partiellement le cas, puisque les décisions des exploitants des fichiers peuvent être portées devant le Tribunal administratif (article 9 LIPD, qui prévoit que les décisions des exploitants d'un fichier refusant de communiquer des renseignement, d'admettre l'opposition ou de procéder à la rectification peuvent être portées devant le Tribunal administratif). L'avant-projet de loi institue une médiation, conduite par le Préposé. Cette médiation est souple afin de permettre aux différends d'être traités avec célérité. Aucune exigence de forme particulière n'est posée, et le Préposé dispose d'une certaine latitude dans le traitement d'une affaire ; il peut par exemple entendre les parties, ou ne se fonder que sur des pièces. Une visite chez l'entité concernée peut également être nécessaire, selon le cas. Si la médiation débouche sur un accord entre les parties, l'affaire est close. Si non, le Préposé émet une recommandation, qu'il notifie aux parties. Au cas où l'autorité compétente n'entend pas suivre la recommandation, elle rend une décision qui pourra être portée devant le Tribunal administratif, soit par l'intéressé, soit par le Préposé lui-même.

La procédure prévue par l'avant-projet de loi s'apparente ainsi à celle instituée par la LInfo, à cette exception près que le Préposé dispose, dans le cadre des demandes fondées sur la présente loi, de la faculté de recourir contre les décisions de l'entité concernée, qui ne suivrait pas sa recommandation. Cela découle des exigences posées par le droit communautaire, en particulier du Protocole additionnel. En revanche, la LInfo ne prévoit pas une telle faculté : seul l'intéressé peut recourir au Tribunal administratif, et ce à l'encontre de la décision rendue initialement, soit avant la saisie du Préposé (article 21 alinéa 1 LInfo).

Article 30 – Détermination écrite

L'entité compétente qui refuse d'accéder aux demandes fondées sur la loi doit fournir au demandeur une détermination écrite. Contrairement à la LInfo, qui impartit un délai de 15 jours au plus à l'autorité pour répondre à une demande d'information (article 12 LInfo), le présent avant-projet de loi ne fixe pas de

délai. L'entité compétente devra cependant traiter la demande aussi rapidement que possible. L'entité compétente sera le plus souvent le responsable du traitement ; il est cependant possible que cela soit d'autres entités (par exemple, le bénéficiaire d'une donnée, dont la communication serait contestée par la personne concernée). Quant à l'intéressé, il peut s'agir soit de la personne concernée, c'est-à-dire la personne dont les données sont traitées, soit d'une autre entité ou d'un tiers, par exemple celle qui requiert la communication de données.

Article 31 – Saisine du Préposé à la protection des données

Le destinataire de la détermination de l'entité compétente peut adresser une demande de médiation au Préposé au cas où il la conteste. Cette saisine doit intervenir dans les vingt jours à compter de la notification de la détermination, ou à la date fixée, le cas échéant, dans la détermination ; cette date ne peut cependant pas être inférieure à vingt jours. Pour la computation des délais, la loi sur la juridiction et la procédure administratives (LJPA, RSV 173.36), qui renvoie au Code de procédure civile, est applicable par analogie (article 32 LJPA). La demande doit être sommairement motivée, ce qui veut dire que l'intéressé n'a pas besoin de mandater un avocat pour l'assister. Il devra cependant joindre à sa demande de médiation la demande qu'il a adressée à l'entité compétente, la détermination de cette dernière, ainsi que les pièces y relatives. Le Préposé se chargera, s'il l'estime nécessaire, de requérir les compléments d'informations utiles.

Article 32 – Médiation

La Préposé doit rechercher une solution compatible avec les dispositions applicables en matière de protection des données, qui puisse satisfaire les parties en présence. La médiation permet aux parties de trouver ensemble une solution, afin de ne porter l'affaire devant les autorités judiciaires qu'en dernier recours. Le Préposé demeure libre de requérir les documents et informations nécessaires à sa tâche ; en ceci, il dispose des moyens qui sont décrits à l'article 41. Si, malgré ses efforts, la conciliation n'aboutit pas, le Préposé émet une recommandation, qu'il notifie aux parties. Cette recommandation doit être rendue dans les trente jours dès la réception de la demande en conciliation.

Article 33 – Décision

Lorsqu'elle reçoit la recommandation du Préposé, l'entité compétente peut décider soit de la suivre, auquel cas l'affaire est réglée, soit de ne pas la suivre, totalement ou partiellement. Elle doit dans ce cas rendre une décision, qu'elle transmet à l'intéressé, ainsi qu'au Préposé, dans les 20 jours qui suivent la

réception de la recommandation. Là encore, la LJPA est applicable en matière de computation des délais.

Article 34 – Gratuité

La saisine du Préposé ne doit pas être entravée pour des questions financières : l'avant-projet de loi prévoit donc que la procédure est gratuite. Ce n'est que si le demandeur est téméraire, ou qu'il dépose une requête abusive, que des émoluments pourront lui être facturés, selon un barème à fixer par le Conseil d'Etat.

Article 35 – Recours au Tribunal administratif

La décision de l'entité compétente peut être portée devant le Tribunal administratif, soit par l'intéressé, soit par le Préposé lui-même. La LJPA est applicable à la procédure de recours.

Article 36 – Exceptions

L'avant-projet de loi prévoit des exceptions au cas où l'autorité compétente est le Conseil d'Etat, le Grand Conseil ou l'ordre judiciaire. En effet, à l'instar de ce qui est prévu par la LInfo (articles 22 à 25), il importe de prévoir des voies de droit particulières pour ces entités. Ces exceptions concerneront toutefois des cas rares, dans la mesure où il est ces entités ne sont en général pas chargée de gérer elles-mêmes un fichier. Cette disposition reprend également l'article 26 LInfo, qui prescrit que les autorités communales statuent sur les demandes concernant leurs activités. Elles pourront, le cas échéant, requérir l'avis du Préposé. Cela entraîne la fin des commissions de recours en matière informatique, existant dans chaque commue. Les décisions des autorités communales pourront être portées devant le Tribunal administratif.

3.9 Chapitre VII Préposé cantonal à la protection des données et à l'information

Article 37 – Désignation

Le Préposé-e cantonal à la protection des données et à l'information est désigné-e par le Conseil d'Etat, pour une durée de 5 ans, renouvelable.

Article 38. – Statut et rattachement

Le Préposé exerce son activité de manière indépendante. Comme indiqué ci-dessus, le Préposé exercera une activité à temps partiel ; par conséquent, il ne pourra pas exercer une autre activité susceptible de porter atteinte à son indépendance.

Article 39 – Surveillance

L'article 31 s'inspire de l'article 27 de la LPD, dont la révision est actuellement en cours, en vue de reconnaître au Préposé fédéral la qualité de recourir contre les décisions rendues par les départements et la Chancellerie suite à ses recommandations (nouvel alinéa 6).

La tâche principale du Préposé est la surveillance de l'application des prescriptions relatives à la protection des données, qu'elles ressortent de la loi sur la protection des données cantonales ou des dispositions spéciales, applicables aux entités cantonales. Il dispose pour cela de moyens qui lui permettent de recueillir toutes les informations dont il a besoin (article 41).

Si, sur la base des faits qu'il a établis, le Préposé estime que les prescriptions relatives à la protection des données ont été violées, il recommande à l'entité concernée, qui sera presque toujours le responsable du traitement, de modifier ou, exceptionnellement de cesser le traitement en question. Sa recommandation est adressée, pour information, au département concerné.

Le Préposé veille ensuite à ce que sa recommandation soit suivie d'effet; si ce n'est pas le cas, il porte l'affaire devant le département ou, s'il s'agit d'une autorité communale, à la Municipalité. S'il s'agit enfin d'une entité énumérée à l'article 2 lit. e et f du présent projet de loi, il s'adressera à la direction de cette entité. Cette autorité rendra une décision, contre laquelle le Préposé pourra recourir. La procédure est régie par la loi sur la juridiction et la procédure administratives.

Article 40 – Autres tâches

Outre la tâche de surveillance, le Préposé accomplit d'autres tâches, énumérées à l'article 32 de l'avant-projet de loi. Ces tâches correspondent de manière générale à celles des autres préposés cantonaux ; elles sont également adaptées au droit communautaire (article 28 Directive 95/46/CE). Le Préposé est tout d’abord chargé de promouvoir, de manière générale, la protection des données au niveau cantonal. Il a également pour tâche de renseigner les responsables de traitement, ainsi que toute personne soumise à la loi, sur les exigences posées en matière de protection des données. Ces exigences peuvent découler soit de la loi cantonale, soit des autres dispositions applicables, le cas échéant. Demeurent cependant réservées les compétences des Préposés fédéraux et cantonaux, s’agissant de la loi fédérale et des lois cantonales. Il doit ensuite renseigner les personnes concernées des droits découlant du présent avant-projet de loi. Il pourra être saisi tant de demandes écrites (courrier, courrier électroniques), qu’orales. A la demande de particuliers ou d'entités soumises à la présente loi, le Préposé pourra être chargé d'officier comme médiateur dans des situations où

des questions de protection des données pourrait poser des problèmes. Son rôle se limitera à fournir des conseils aux personnes et entités concernées, il ne peut pas rendre de décision formelle. Afin de veiller au respect des prescriptions régissant la protection des données, le Préposé doit être impliqué dans tous les actes normatifs impliquant le traitement de données personnelles. Sont visés ici non seulement les lois et règlements élaborés par l'administration, mais également les directives et autres actes prévoyant le traitement de données personnelles. Le Préposé doit également tenir le registre des fichiers prévu par l'avant-projet de loi ; il s'assure pour cela auprès des responsables de traitement que ces derniers fournissent tous les renseignements nécessaires à la tenue du registre. Cette tâche sera l'une des premières qu'il aura à accomplir, dès son entrée en fonction (article 40). Enfin, le Préposé devra collaborer avec les autres entités chargées de la protection des données, que cela soit dans les autres cantons suisses, à la Confédération ou encore à l'étranger, pour les questions relevant de la protection des données. Cette tâche s'inscrit en particulier dans le cadre de la mise en œuvre des Accords de Schengen et de Dublin.

Article 41 – Pouvoir

Pour pouvoir accomplir sa mission, le Préposé doit disposer d'un large accès aux données personnelles. Afin de garantir le respect de la loi, il doit pouvoir rendre, préalablement à la mise en œuvre d'un fichier, un avis sur la conformité de ce dernier avec les règles applicables à la protection des données. Le Préposé doit également être en mesure d'intervenir auprès du responsable du traitement, dans l'hypothèse où la personne concernée fait valoir un intérêt digne de protection s'opposant au traitement de données personnelles. Ce pouvoir, qui peut avoir de sérieuses conséquences pour le responsable du traitement ou pour les bénéficiaires, ne devra être exercé qu'en dernier recours et de manière exceptionnelle.

Article 42 – Obligation de renseigner

Le Préposé doit pouvoir compter sur la collaboration des responsables de traitement ; l'avant-projet de loi prévoit donc que ces derniers fournissent tous les renseignements nécessaires. Un accès aux locaux du responsable du traitement est également prévu, à l'instar de ce qui est prévu pour d'autres entité chargées de contrôle au sein de l'Etat (CCF, CdC, etc.). Le Préposé est tenu au secret de fonction, derrière lequel les responsables de traitement ne peuvent se retrancher pour ne pas lui fournir de renseignements.

L'obligation de renseigner s'étend également à tous les tiers auxquels les responsables de traitement ont confié le traitement de données personnelles.

Article 43 – Rapport

Le rapport annuel élaboré par le Préposé poursuit plusieurs objectifs. Premièrement, il permet d'avoir un aperçu des activités déployées par ce dernier pendant l'année. De plus, dans la mesure où il est public, le rapport permet de promouvoir la protection des données en donnant des exemples pratiques dans lesquels la protection des données trouve application. Le Préposé pourra également rapporter sur ses interventions auprès des responsables de traitement et, le cas échéant, indiquer si elles ont été suivies d'effets ou non.

En plus de son rapport annuel, le Préposé peut établir un rapport spécial, sur demande du Grand Conseil, du Conseil d'Etat ou de son propre chef. Seules des circonstances très particulières peuvent cependant conduire à l'élaboration d'un rapport spécial ; en effet, le Préposé s'efforcera de faire figurer, dans le rapport annuel, l'ensemble de ses activités.

3.10 Chapitre IX Violation de la loi

Article 44 Violation de la loi

Le personnel de l'Etat de Vaud, ainsi que les personnes auxquelles l'Etat de Vaud a confié l'exécution de certaines tâches, sont tenus par l'article 19 LInfo, qui interdit de divulguer des informations ou des documents officiels dont ils ont eu connaissance dans l'exercice de leur fonction, et qui doivent rester secrets en raison de la loi ou d'un intérêt public ou privé prépondérant. Les données personnelles ou sensibles traitées par les personnes soumises au présent avant-projet de loi doivent, par définition, rester secrètes, sauf si leur divulgation ressort de la loi ou découlant de l'exécution de tâches légales. Eu égard au champ d'application de l'avant-projet de loi, il convient de prévoir une disposition interdisant à toutes les entités qui y sont soumises de révéler de manière illicite les données personnelles ou sensibles qui leur ont été transmises.

3.11 Chapitre X Dispositions transitoires

Article45 – Exécution

Le Conseil d'Etat édicte, s'il l'estime nécessaire, des dispositions d'application du présent avant-projet de loi.

Article 46 – Base légale

Le traitement des données personnelles effectué par les entités soumises au présent avant-projet de loi doit s'y conformer dans les 5 ans qui suivent son entrée en vigueur.

Article 47 – Registre des fichiers

La constitution du registre des fichiers devra se faire dans les deux ans qui suivent l'entrée en vigueur de la loi. Chaque responsable du fichier sera amené à fournir la liste exhaustive des fichiers qu'il exploite au Préposé, dont l'une des premières tâches sera de prendre les dispositions relatives à la constitution du registre, ainsi que de sa mise en ligne.

Article 48 – Abrogation de la loi sur les fichiers informatiques et la protection des données personnelles

Le présent avant-projet de loi abroge la LIPD.

4. LOI MODIFIANT LA LOI SUR L'INFORMATION

Comme indiqué ci-dessus, l'avant-projet de loi sur la protection des données prévoit d'instituer un Préposé qui sera à la fois chargé de la protection des données et de l'information. Cela entraîne une modification de la LInfo, en particulier de ses articles 2 et 21. En effet, afin d'assurer une cohérence entre la loi sur la protection des données et la loi sur l'information, il convient de soumettre les mêmes entités au champ de contrôle des deux lois.

L'autre modification à la LInfo consiste à harmoniser la procédure applicable à l'accès à un document et celle fondée sur la loi sur la protection des données (cf. chapitre 1.3 ci-dessus). Tout d'abord, la procédure de médiation, à laquelle l'intéressé peut ou non avoir recours (l'article 21 LInfo prévoit en effet que l'intéressé peut choisir de saisir la commission restreinte en vue d'une médiation, ou porter l'affaire devant le Tribunal administratif), devient désormais nécessaire avant tout recours au Tribunal administratif. Cette modification vise à privilégier la médiation, qui présente plusieurs avantages, tels que la célérité, la recherche d'une solution convenant aux deux parties. La médiation sera du ressort du Préposé, qui remplacera en cela la commission restreinte instituée par la LInfo.

Cette charge de travail ne devrait pas être trop conséquente pour le Préposé, dans la mesure où la commission restreinte qu'il remplace n'a eu à offrir sa médiation que une à deux fois par année depuis l'entrée en vigueur de la LInfo. Le règlement de la LInfo devra également être adapté, l'ensemble des compétences de la commission restreinte devant être transférées au Préposé à la

protection des données et à l'information. Ce transfert de compétence aura également des répercussions au niveau de la Chancellerie, qui assure pour l'instant, notamment, le secrétariat de la commission permanente.

Enfin, un nouveau chapitre, précisant les devoirs du Préposé en matière d'information, est inséré dans la loi.

5. LOI MODIFIANT LA LOI SUR LA STATISTIQUE CANTONALE

Les statisticiens ont de plus en plus recours à des données provenant de registres administratifs, qui présentent un potentiel d'exploitation statistique intéressant. Cela a notamment mené la Confédération à élaborer une loi sur l'harmonisation des registres, qui vise à simplifier la collecte de données à des fins statistiques en assurant l'harmonisation de registres officiels de personnes, ainsi que l'échange des données personnelles de ces registres. Cet avant-projet de loi entraîne notamment la modification de la loi sur la statistique fédérale, par l'introduction d'un article 14a, relatif à l'appariement des données.

Dans la mesure où cela concerne la protection des données, le Conseil d'Etat propose d'adapter la loi sur la statistique en y insérant une disposition analogue à ce qui est prévu au niveau fédéral.

En cas d'appariement des données, ces dernières doivent bénéficier d'une protection particulière, dans la mesure où elles concernent des domaines tels que la santé ou la protection sociale et qu'elles sont dès lors considérées comme "sensibles" au sens de l'avant-projet de loi sur la protection des données. En outre, l'appariement de données non qualifiées de sensibles peut déboucher sur des profils de la personnalité.

Aussi est-il prévu que l'autorité compétente au sens de la loi, soit le Service cantonal de recherche et d'informations statistiques, soit autorisé à apparier, à des fins statistiques, de recherche et de planification, les données qu'il saisit dans le cadre de l'une des activités statistiques prévues par la loi. Dès que ses travaux le lui permettent, le SCRIS doit rendre ces données anonymes.

S'agissant des données sensibles, elles ne peuvent être appariées que temporairement, et ce uniquement à des fins statistiques. Ceci est également le cas pour les données permettant d'établir des profils de la personnalité. Les autres dispositions, relatives notamment à la sécurité des données, sont pour le surplus applicables.

6. CONSEQUENCES DU PROJET DE LOI

6.1 Incidences financières

La mise en place d'une autorité chargée de la protection des données va générer des dépenses qu'il est possible, au stade actuel, d'estimer à environ 150'000.- francs. Ce montant comprend la rétribution du Préposé cantonal (qui travaillera à temps partiel), d'un secrétariat (également à temps partiel), la location de locaux, ainsi que les frais relatifs à la publication du rapport.

Ces frais sont en partie compensés par la diminution du budget du Secrétariat général du Département des finances, qui ne sera plus en charge de la protection des données, ainsi que de celle du budget de la Chancellerie, qui n'accordera plus d'indemnités aux membres de la commission restreinte. Cette compensation est évaluée à près d'un sixième du budget du Préposé cantonal, tel qu'estimé ci-dessus.

6.2 Charges nouvelles

L'avant-projet de loi sur la protection des données entraîne des charges relatives, exclusivement, au nouveau Préposé et à son activité. Il convient tout d'abord de relever que certaines de ses tâches attribuées ne constituent pas des charges nouvelles puisqu'elles sont assumées à l'heure actuelle par le Secrétariat général du Département des finances. Il s'agit de l'information et des renseignements relatifs aux exigences posées par la loi (article 40 lit. b et c), à la consultation dans le cadre d'élaboration de lois et autres normes impliquant le traitement de données personnelles (article 40 lit. e) et à la tenue du registre des fichiers (article 40 lit. g). Ainsi, ne sont concernées par l'article 163 alinéa 2 Cst-VD que les charges découlant du statut du Préposé, ainsi que des tâches énumérées à l'article 39 (surveillance en général) et 40, lit. a, d, f et h.

L'institution d'une autorité indépendante, chargée de veiller au respect des dispositions applicables à la protection des données, découle du droit supérieur, soit en particulier du Protocole additionnel à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le message du Conseil fédéral prévoit en effet que les cantons suisses doivent adapter leur législation à ce Protocole additionnel.[42] Le protocole additionnel devrait être ratifié par le Conseil fédéral fin 2007, pour entrer en vigueur en avril 2008. En ce qui concerne les tâches du Préposé, elles découlent donc du Protocole additionnel, mais également de la Directive 95/46/CE, qui fait partie intégrante de l'acquis de Schengen, auquel

[42] FF 2003, p. 1959

les cantons doivent également se conformer dans un délai relativement court (il est en effet prévu que les contrôles entrepris auprès des cantons pour vérifier si leurs législations remplissent les conditions posées par les Accords de Schengen et de Dublin seront effectués fin 2006 ou courant 2007). Les attributions du Préposé, énumérées à l'article 28 de la Directive précitée, sont en effet reprises dans l'avant-projet de loi.

Dans son 2ème avis de droit, le Professeur Auer s'est prononcé sur la question des charges reportées par la Confédération sur les cantons, en citant deux exemples : celui du "paquet financier", ainsi que la répartition des tâches entre la Confédération et les cantons (RPT) (2ème avis de droit, pp. 7 et 8). Pour examiner s'il s'agit de charges nouvelles ou non, le Professeur Auer examine si les cantons disposent d'une marge de manœuvre pour la mise en vigueur des mesures imposées par la Confédération. Il applique ainsi les principes généraux dégagés par la jurisprudence pour qualifier les charges de nouvelles ou non, sans fournir de réponses spécifiques aux charges reportées par la Confédération sur les cantons.

Il convient dès lors de vérifier si, par rapport au Protocole d'accord et à la Directive 95/46/CE, le canton dispose d'une marge de manœuvre ou non. A la lecture de l'art. 1 du Protocole additionnel, il apparaît que le statut et les compétences de l'autorité, qui doit être indépendante, sont énumérées de manière relativement précise. S'agissant tout d'abord de l'indépendance du Préposé, elle repose sur les critères habituellement appliqués dans ce domaine (cf. chapitre 2.9 ci-dessus). En prévoyant un rattachement à la Chancellerie, l'avant-projet de loi assure une indépendance au Préposé, sans instituer une entité totalement distincte de l'Etat, avec les coûts que cela pourrait entraîner. De surcroît, en instituant un Préposé, travaillant à temps partiel, en lieu et place d'une commission composée de plusieurs membres rétribués à la commission, l'avant-projet de loi favorise la solution engendrant le moins de frais pour l'Etat. Pour ce qui est des compétences du Préposé, l'avant-projet de loi est en tous points adapté aux Protocole additionnel et à la Directive 95/46/CE. La surveillance générale prévue à l'article 39, avec les moyens prévus à l'article 41 (droit d'accès, préavis préalable, cessation de traitement), correspondent à ce qui est prévu à l'article 1 du Protocole et à l'article 28 de la Directive 95/46/CE. S'agissant des autres tâches (promotion de la protection des données, médiation, collaboration), elles correspondent à ce qui est prévu à l'article 28 de la Directive 95/46/CE. Le rapport d'activité du Préposé découle enfin de l'article 28 ch. 5 de la Directive précitée.

Aussi seule la compétence relative à la vidéo-surveillance (article 40 lit. f) constitue-t-elle une charge ne découlant pas de la mise en œuvre des différentes normes européennes. Cette tâche ne devrait cependant que constituer une infime

partie de l'activité déployée par le Préposé. S'agissant des activités que le Préposé devra effectuer en matière d'information au public, elles correspondent à celles assumées à l'heure actuelle par la Commission restreinte. Par conséquent, elles ne constituent pas des charges nouvelles.

Il apparaît dès lors que les charges nouvelles entraînées par l'avant-projet de loi découlent de l'adaptation du droit cantonal au droit supérieur. Ce droit supérieur s'impose aux cantons, qui ne disposent pas de marge de manœuvre, ni dans l'adaptation de leur législation au droit communautaire, ni dans le délai imparti pour ce faire (2008). En outre, les solutions retenues dans l'avant-projet sont celles qui présentent les charges financières les moins élevées. Par conséquent, le DFIN n'a pas à proposer de compensation aux charges découlant de l'avant-projet de loi. Pour ce qui est des autres charges découlant de l'avant-projet de loi, elles ne peuvent être qualifiées de nouvelles, car elles correspondent à ce qui est assuré à l'heure actuelle, d'une part par le Secrétariat général du Département des finances s'agissant de la protection des données, d'autre part par la Chancellerie, s'agissant de l'information au public.

6.3 Conséquences sur le personnel

Comme indiqué ci-dessus, le présent avant-projet entraîne la création de deux nouveaux postes de travail : un-e Préposé-e et un-e secrétaire, qui travailleront à temps partiel, représentant un ETP au total qui sera compensé.

6.4 Conséquences sur l'environnement

Aucune.

6.5 Conséquences sur les communes

Toutes les communes vaudoises sont soumise à la LIPD ; elles ont en outre adopté un règlement sur les fichiers informatiques et la protection des données personnelles : ces derniers seront abrogés à l’entrée en vigueur de la présente loi. Les commissions de recours en matière informatique, instituées par chacune des communes vaudoises, seront supprimées, dans la mesure où les autorités communales statueront sur les demandes concernant leurs activités.

6.6 Conséquences sur la mise en œuvre de la nouvelle Constitution

L'avant-projet de loi présenté est conforme à la nouvelle Constitution. Il met en œuvre l'article 15 alinéa 2 Cst-VD. Il s’inscrit dans la planification des travaux législatifs de mise en œuvre de la nouvelle Constitution (Rapport du Conseil d’Etat au Grand Conseil sur l’état des travaux de mise en œuvre de la nouvelle Constitution 257 (R. 8/05, pp. 10 et 29).

6.7 Conformité au droit communautaire

Pour les raisons invoquées ci-dessus (chapitre 1.1.2), le présent avant-projet se conforme, dans une large mesure, au droit communautaire.

AVANT-PROJET DE LOI

sur la protection des données personnelles

LE GRAND CONSEIL DU CANTON DE VAUD

vu l'article 15 de la Constitution cantonale du 14 avril 2003,

vu le projet de loi présenté par le Conseil d'Etat,

décrète

CHAPITRE PREMIER

But, champ d'application et définitions

But

Article premier. – La présente loi vise à protéger les personnes contre l'emploi abusif des données personnelles les concernant.

Champ d'application

Art. 2. – La présente loi s'applique à tout traitement de données des personnes physiques et des personnes morales, contenues dans des fichiers, quel que soit leur mode de traitement et quels que soient les moyens et procédés utilisés.

Sont soumis à la présente loi les entités suivantes :

a) le Grand Conseil ;

b) le Conseil d'Etat et son administration ;

c) l'Ordre judiciaire et son administration ;

d) les communes, ainsi que les ententes, associations, fédérations, fractions et agglomérations de communes ;

e) les personnes physiques et morales auxquelles le canton ou une commune confie des tâches publiques.

La présente loi ne s'applique pas :

a) aux délibérations du Grand Conseil et des conseils généraux et communaux ;

b) aux procédures civiles, pénales ou administratives, à l'exception des procédures administratives de première instance ;

c) aux personnes physiques ou morales visées sous lettre e) de l'al. 1 accomplissant des activités relevant de droit privé;

d) aux outils de travail hautement personnel.

Définitions

Art. 3. – On entend par :

1) *Données personnelles*, toutes informations qui se rapportent à une personne identifiée ou identifiable ;

2) *Données sensibles*, toute donnée personnelle se rapportant :

(i) aux opinions ou activités religieuses, philosophiques, politiques ou syndicales ;

(ii) à la santé, la sphère intime ou l'appartenance à une race ;

(iii) aux mesures d'aides sociales ou d'assistance ;

(iv) aux poursuites ou sanctions pénales et administratives.

3) *Profil de la personnalité*, assemblage de données qui permet de d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique ;

4) *Personnes concernées*, toute personne physique ou morale au sujet de laquelle les données sont traitées ;

5) *Traitement de données personnelles*, toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données personnelles, notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

6) *Communication*, fait de rendre des données accessibles,

notamment de les transmettre, les publier, d'autoriser leur consultation ou fournir des renseignements ;

7) *Fichier*, tout ensemble structuré de données personnelles accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

8) *Responsable du traitement*, la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine le contenu, ainsi que les finalités du fichier ;

9) *Sous-traitant*, personne physique ou morale, l'autorité publique ou tout autre organisme qui traite des données personnelles pour le compte du responsable du traitement ;

10) *Consentement de la personne concernée*, toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données personnelles la concernant fasse l'objet d'un traitement ;

11) *Procédure d'appel*, mode de communication automatisé des données par lequel les destinataires décident eux-mêmes de la communication des données, moyennant une autorisation du responsable du traitement ;

12) *Destinataire*, personne physique ou morale, de droit privé ou de droit public, qui reçoit communication de données, qu'il s'agisse ou non d'un tiers ; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des destinataires ;

13) *Entités*, les entités décrites à l'article 2 alinéa 2 de la présente loi ;

14) *Loi au sens formel*, les lois au sens formel sont celles qui sont adoptées par le Grand Conseil et sujettes au référendum ou, s'agissant des domaines relevant de l'autonomie communale, les règlements adoptés par les conseils généraux et communaux.

CHAPITRE II

Dispositions générales

Sections I

Principes

Légalité

Art. 4. – Les données personnelles ne peuvent être traitées que s'il existe une base légale ou si leur traitement sert à l'accomplissement d'une tâche légale.

Les données sensibles ne peuvent être traitées que si :

a) une loi au sens formel le prévoit expressément,

b) l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument, ou

c) la personne concernée y a consenti ou a rendu ses données accessibles à tout un chacun.

Finalité

Art. 5. – Les données ne doivent être traitées que dans le but indiqué lors de leur collecte, tel qu'il ressort de la loi ou des circonstances.

Proportionnalité

Art. 6. – Le traitement des données personnelles doit être conforme au principe de la proportionnalité.

Transparence

Art. 7. – La collecte des données personnelles doit être reconnaissable pour la personne concernée.

Lorsque le traitement de données personnelles requiert le consentement de la personne concernée, ce dernier n'est donné valablement que s'il est donné librement, après que la personne a été informée. Ce consentement doit être explicite lorsque le traitement porte sur des données sensibles.

Exactitude

Art. 8. – Les entités soumises à la présente loi s'assurent que les données personnelles traitées sont exactes.

Sécurité

Art. 9. – Le responsable du traitement prend les mesures appropriées pour garantir la sécurité des fichiers et des données personnelles, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite.

Conservation

Art. 10. – Les données personnelles doivent être détruites ou rendues anonymes dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées.

Demeurent réservées les dispositions légales spécifiques à la conservation des données, en particulier à leur archivage, ou effectuées à des fins historiques, statistiques ou scientifiques.

Section II

Traitement des données personnelles

Devoir d'informer

Art. 11. – Le responsable du traitement informe la personne concernée de toute collecte des données personnelles la concernant, à moins qu'elle n'ait été informée préalablement.

Les informations fournies à la personne concernées sont les suivantes :

a) l'identité du responsable du traitement ;

b) la finalité du traitement pour lequel les données sont collectées ;

c) au cas où la communication des données est envisagée, les catégories des destinataires des données ;

d) le droit d'accéder aux données ;

e) les conséquences découlant du refus de sa part de fournir les données personnelles demandées.

Si les données ne sont pas collectées auprès de la personne concernée, le responsable du traitement doit fournir à cette dernière les informations énumérées à l'alinéa précédent, au plus tard lors de l'enregistrement des données, à moins que cela ne s'avère impossible, ne nécessite des efforts disproportionnés ou que l'enregistrement ou la communication ne soient expressément prévus par la loi.

Devoir d'informer lors de décisions individuelles automatisées

Art. 12. – Lorsqu'une décision produisant des effets juridiques pour la personne concernée, ou l'affectant de manière significative, est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, la personne concernée doit être expressément informée.

Restriction du devoir d'information

Art. 13. – Le responsable du traitement peut refuser ou restreindre l'information visée à l'article 11, voire en différer l'octroi, dans la mesure où :

a) une loi au sens formel le prévoit, ou

b) les intérêts prépondérants d'un tiers l'exigent.

Le responsable du traitement définit à l'article 2 alinéa 2 lettres a à c peut en outre refuser ou restreindre l'information demandée, voire en différer l'octroi, dans la mesure où :

a) un intérêt public prépondérant l'exige, ou

b) l'information ou la communication du renseignement risque de compromettre une instruction pénale ou une autre procédure d'instruction.

Le responsable du traitement définit à l'article 2 alinéa 2 lettre d et e peut en outre refuser ou restreindre l'information demandée, voire en différer l'octroi, dans la mesure où ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à un tiers.

Dès que le motif justifiant la restriction du devoir d'information disparaît, le responsable du traitement doit fournir l'information, à moins que cela ne soit impossible ou ne nécessite des efforts disproportionnés.

Communica-tion

Art. 14. – Les données personnelles peuvent être communiquées par les entités soumises à la présente loi lorsque :

a) une disposition légale le prévoit ;

b) le requérant établit qu'il en a besoin pour accomplir ses tâches légales ;

c) la personne concernée a expressément donné son accord ou que les circonstances permettent de présumer ledit accord ;

d) la personne concernée a rendu les données personnelles accessibles à tout un chacun ;

e) le destinataire rend vraisemblable que la personne concernée ne refuse son accord que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes ; dans ce cas, la personne concernée est invitée, dans la mesure du possible, à se prononcer, préalablement à la communication des données.

La communication par procédure d'appel n'est possible que si elle est expressément prévue dans une loi au sens formel ou un règlement. Les données sensibles ne peuvent être communiquées par procédure d'appel que si une loi au sens formel le prévoit.

Modalité

1. Forme et consultation

Art. 15. – La demande portant sur la communication de données personnelles n'est soumise à aucune exigence de forme. Elle doit contenir toutefois les indications suffisantes pour permettre d'identifier la donnée concernée.

La communication des données a lieu sur place ou se fait par écrit, sauf disposition contraire.

Avec l'accord du requérant, la communication peut également se faire par oral.

2. Gratuité

Art. 16. – La communication des données est, en règle général, gratuite.

Le responsable du traitement qui répond à la demande peut percevoir un émolument :

a) lorsque la communication requiert un travail important ;

b) en cas de demandes répétitives ;

c) lorsqu'une copie est demandée.

Le Conseil d'Etat fixe le tarif des émoluments.

Communication transfrontière de données

Art. 17. – Le transfert vers un pays tiers de données personnelles faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement, ne peut avoir lieu que si le pays tiers en question assure un niveau de protection adéquat.

L’alinéa précédent n’est pas applicable :

a) si la personne concernée a donné son consentement ; s’il s’agit de données sensibles, le consentement doit être explicite ;

b) si le transfert de données est nécessaire à l’exécution d’un contrat entre la personne concernée et le responsable du traitement ou à l’exécution de mesures pré-contractuelles prises à la demande de la personne concernée ;

c) si le transfert est nécessaire à la conclusion ou à l’exécution d’un contrat conclu ou à conclure, dans l’intérêt de la personne concernée, entre le responsable du traitement et un tiers ;

d) si le transfert est nécessaire à la sauvegarde de l’intérêt vital de la personne concernée ;

e) si le transfert intervient d’un registre public qui, en vertu de dispositions légales ou réglementaires, est destiné à l’information du public ou de toute personne justifiant d’un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier ;

f) si des garanties suffisantes, notamment contractuelles, permettent d’assurer un niveau de protection adéquat à l’étranger.

Traitement des données par un tiers

Art. 18. – Le traitement de données peut être confié à un tiers aux conditions suivantes :

a) le traitement par un tiers est prévu par la loi ou par un contrat ;

b) le responsable du traitement est légitimé à traiter lui-même les données concernées ;

c) aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Le tiers est responsable de la sécurité des données qu'il traite.

Chapitre III Fichiers

Registre des fichiers

Art. 19. – Le Préposé cantonal à la protection des données et à l'information (ci-après : le Préposé) tient un registre des fichiers, qui est public et accessible en ligne.

Le Conseil d'Etat édicte les règles applicables à la tenue du registre.

Annonce

Art. 20. – Les entités soumises à la présente loi sont tenues d'informer le Préposé lors de tout projet visant à constituer un nouveau fichier contenant des données personnelles.

Les fichiers ne peuvent être opérationnels avant d'être enregistrés par le Préposé.

Le Conseil d'Etat fixe les renseignements à fournir lors de l'annonce de fichier.

Chapitre IV Vidéo surveillance

Conditions

Art. 21. – Un système de vidéo surveillance peut être installé sur le domaine public cantonal ou communal, moyennant le respect des principes et prescriptions de la présente loi.

Il doit notamment se conformer aux principes suivants :

a) légalité : seule une loi au sens formel peut autoriser l'installation d'un système de vidéo surveillance ;

b) finalité : les images enregistrées par le système de vidéo surveillance ne peuvent être utilisées qu'aux fins fixées dans la loi qui l'institue ;

c) proportionnalité : l'installation du système de vidéo surveillance doit apparaître comme le seul moyen propre à atteindre le but poursuivi. Toutes les mesures doivent être prises pour limiter les atteintes aux personnes concernées ;

d) conservation : la durée de conservation des données ne peut excéder 24 heures, sauf si la donnée est nécessaire à des fins de preuves, ceci conformément à la finalité poursuivie par le système de vidéo surveillance.

Tout projet tendant à l'installation de vidéo surveillance doit être annoncé au Préposé.

Le système de vidéo surveillance ne peut être mis en fonction avant l'accord du Préposé.

Le Conseil d'Etat précise les conditions précitées.

Indications

Art. 22. – Le responsable du traitement doit indiquer de manière visible, aux abords directs du système de vidéo surveillance :

a) le but de la vidéo surveillance ;

b) l'emplacement du système de vidéo surveillance et le champ vidéo surveillé ;

c) les coordonnées du responsable du traitement ;

d) les droits d'accès aux images enregistrées.

Chapitre V Statistiques, planification et recherche

Art. 23. – Les entités soumises à la présente loi sont en droit de traiter des données personnelles à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, aux conditions suivantes :

a) elles sont rendues anonymes dès que le début de leur traitement le permet ;

b) le destinataire ne communique les données à des tiers qu'avec le consentement de l'entité qui les lui a transmises ;

c) les résultats du traitement sont publiés sous une forme ne permettant pas d'identifier les personnes concernées.

Les articles 4 alinéa 2, 5, 14 de la présente loi ne sont pas applicables.

La loi sur la statistique cantonale[43] est pour le surplus applicable.

Chapitre VI Droits de la personne concernée

Consultation des fichiers

Art. 24. – Toute personne a, en tout temps, libre accès aux fichiers la concernant.

Elle peut également requérir du responsable du traitement la confirmation que des données la concernant ne sont pas traitées.

La personne qui fait valoir son droit doit justifier de son identité.

Modalités

Art. 25. – Les modalités applicables à la communication des données (articles 15 et 16 de la présente loi) s'appliquent également à la consultation des fichiers.

Restrictions

Art. 26. – Le responsable du traitement peut refuser de fournir les renseignements demandés ou restreindre leur consultation, si :

a) la loi le prévoit expressément ;

b) un intérêt public important l’exige ;

c) un intérêt de tiers particulièrement digne de protection le commande, ou

d) la protection de la personne concernée ou des droits et liberté de tiers le requièrent.

Les données médicales peuvent être communiquées au médecin consulté par la personne concernée.

Dès que le motif justifiant la restriction du devoir d'accès disparaît, le responsable du traitement doit fournir l’information, à moins que cela ne soit impossible ou ne nécessite des efforts disproportionnés.

---

[43] RSV 431.01

Droit d'opposition

Art. 27. – Toute personne a le droit de s'opposer à ce que les données personnelles la concernant soient communiquées, si elle fait valoir un intérêt légitime.

Le responsable du traitement rejette ou lève l'opposition :

a) si la communication est expressément prévue par une disposition légale ;

b) si la communication est indispensable à l'accomplissement des tâches légales du bénéficiaire.

Autres droits

Art. 28. – Toute personne ayant un intérêt légitime peut exiger du responsable du traitement qu'il :

a) s'abstienne de procéder à un traitement illicite de données ;

b) supprime les effets d'un traitement illicite de données ;

c) constate le caractère illicite d'un traitement de données ;

d) répare les conséquences d'un traitement illicite de données.

Le cas échéant, il peut demander au responsable du traitement de :

a) rectifier, détruire les données ou les rendre anonymes ;

b) publier ou communiquer à des tiers la décision ou la rectification.

Si ni l'exactitude, ni l'inexactitude d'une donnée ne peut être établie, le responsable du traitement ajoute à la donnée la mention de son caractère litigieux.

Réponse du responsable du traitement

Art. 29. – Le responsable du traitement indique par écrit à la personne concernée les motifs l'ayant conduit à refuser de donner suite aux demandes fondées sur les articles 24 à 28 de la présente loi.

Chapitre VII Prétention, médiation et procédure

Détermination rendue par l'entité compétente

Art. 30. – Pour toute demande fondée sur la présente loi, l'entité compétente doit indiquer par écrit à l'intéressé les motifs l'ayant conduit à ne pas y donner suite.

L'entité compétente adresse une copie de sa détermination au Préposé.

Saisine du Préposé

Art. 31. – L'intéressé peut saisir le Préposé par une demande en médiation sommairement motivée, dans un délai de vingt jours dès la notification de la détermination. Passé ce délai, la détermination devient définitive.

Médiation

Art. 32. – Dès qu'il est saisi d'une demande en médiation, le Préposé la notifie à l'entité compétente.

Le Préposé s'efforce d'amener les parties à un accord. Il dispose à cet effet des moyens décrits à l'article 41 de la présente loi.

Si la médiation aboutit, l'affaire est classée.

Si une procédure de médiation n'aboutit pas à un accord qui satisfait les deux parties, le Préposé prend position sur l'affaire et donne sa recommandation écrite à l'entité compétente et à l'intéressé.

Décision

Art. 33. – L'entité compétente rend une décision dans les dix jours à compter de la date de réception de la recommandation.

Elle notifie sa décision à l'intéressé et au Préposé.

Gratuité

Art. 34. – La procédure est gratuite.

Un émolument peut être perçu en cas de demande abusive.

Le Conseil d'Etat fixe le tarif des émoluments.

Recours

Art. 35 – La décision de l'entité compétente est sujette à recours au Tribunal administratif.

Le refus de statuer ou le dépassement du délai prescrit à l'article 34 alinéa 3 sont assimilés à une décision.

La procédure de recours est régie par la loi sur loi sur la juridiction et

la procédure administratives (RSV 173.36).

Exceptions

Art. 36. – Lorsque l'entité compétente est le Conseil d'Etat, il statue définitivement sur les demandes.

Lorsque l'entité compétente est le Grand Conseil, le bureau du Grand Conseil statue définitivement sur les demandes fondées sur la présente loi.

Lorsque l'entité compétente est une autorité ou un office judiciaire, ses décisions sont susceptibles de recours au Tribunal cantonal.

Lorsque l'entité compétente est le Tribunal cantonal ou le Tribunal administratif, ces derniers statuent définitivement.

Les autorités communales statuent sur les demandes concernant leurs activités. Elles rendent une décision susceptible de recours au Tribunal administratif dans les vingt jours à compter de sa notification.

Chapitre VIII Préposé cantonal à la protection des données et à l'information

Désignation

Art. 37. – Le Préposé est désigné par le Conseil d'Etat, pour une période de 5 ans.

Son mandat est renouvelable.

Statut et rattache-ment

Art. 38. – Le Préposé exerce son activité de manière indépendante.

Il est rattaché administrativement à la Chancellerie.

Le Préposé est tenu au secret de fonction.

Tâches

1. Surveil-lance

Art. 39. – Le Préposé surveille l'application des prescriptions relatives à la protection des données.

A cette fin, il dispose des moyens prévus à l'article 41 de la présente loi.

S'il estime que les prescriptions sur la protection des données ont été violées, le Préposé transmet une recommandation à l'entité concernée, en vue de modifier ou cesser le traitement concerné.

Si la recommandation du Préposé n'est pas suivie, ce dernier peut

porter l'affaire devant le département ou l'entité concernée, pour décision.

Le Préposé peut recourir contre la décision rendue conformément à l'alinéa précédent, ainsi que contre la décision rendue par l'autorité compétente suite à la médiation (article 34). La loi sur la juridiction et la procédure administratives[44] est applicable.

2. Autres tâches

Art. 40. – Outre la surveillance mentionnée ci-dessus, le Préposé:

a) promeut la protection des données dans le canton ;

b) informe les responsables de traitement sur les exigences posées en matière de protection des données ;

c) renseigne les personnes concernées sur les droits découlant de la présente loi ;

d) offre sa médiation, sur demande des responsables de traitement et des personnes concernées, afin de résoudre des cas soumis à la présente loi (article 34);

e) est consulté lors de l'élaboration de loi, règlement, directive ou autre norme impliquant le traitement de données personnelles ;

f) est consulté dans le cadre de l'installation de vidéosurveillance ;

g) tient à jour le Registre des fichiers institué à l'article 19 de la présente loi ;

h) collabore avec les autres autorités compétentes en matière de protection des données des autres cantons, de la Confédération ou de l'étranger.

Moyens

Art. 41. – Dans le cadre de ses tâches, le Préposé peut :

a) accéder aux données faisant l'objet d'un traitement et recueillir toutes les informations nécessaires à

---

[44] RSV 173.36

l’accomplissement de ses tâches ;

b) rendre un préavis préalablement à la mise en œuvre d’un fichier, conformément à l’article 20 et assurer un avis y relatif approprié ;

c) si des intérêts dignes de protection de la personne concernée le requièrent, demander au responsable du traitement de restreindre ou cesser immédiatement, de manière temporaire ou définitive, le traitement de données personnelles.

Obligation de renseigner

Art. 42. – Le responsable du traitement est tenu d’assister le Préposé dans l’accomplissement de ses tâches. A cet effet, il lui fournit les informations ou pièces nécessaires et le laisse accéder à ses locaux.

Le secret de fonction ne peut être opposé au Préposé.

Les tiers sont également tenus de fournir les renseignements requis par le Préposé.

Rapport

Art. 43. – Le Préposé établit chaque année un rapport d’activité.

Ce rapport est public.

Le Préposé peut établir, en tout temps, un rapport spécial, d’office ou sur demande du Grand Conseil ou du Conseil d’Etat.

Chapitre XIX Violation de la loi

Violation du devoir de discrétion

Art. 44. – Toute personne ayant révélé intentionnellement, d’une manière illicite, des données personnelles ou sensibles qui ont été portées à sa connaissance dans l’exercice de sa fonction, sera punie d'une amende.

Est passible de la même peine la personne ayant révélé intentionnellement, d’une manière illicite, des données personnelles ou sensibles portées à sa connaissance dans le cadre des activités qu’elle exerce pour le compte de personnes soumises à l’obligation de garder le secret.

L’obligation de discrétion persiste au-delà de la fin des rapports de

travail.

Chapitre X Dispositions transitoires

Base légale

Art. 45. – Le Conseil d'Etat édite les dispositions nécessaires à l'application de la loi.

Mise en oeuvre

Art. 46. – Dans les cinq ans suivant son entrée en vigueur, tout traitement des données doit se conformer à la présente loi, notamment en matière de légalité.

Dans l'année qui suit l'entrée en vigueur de la présente loi, les responsables du traitement annoncent les fichiers au Préposé.

Registre des fichiers

Art. 46. – Le Registre du fichier est établi dans les deux ans suivant l'entrée en vigueur de la présente loi.

Abrogation de la LIPD

Art. 47. – La loi du 25 mai 1981 sur les fichiers informatiques et la protection des données personnelles est abrogée.

***Art. 2.* –** Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale et en fixera, par voie d'arrêté, la date d'entrée en vigueur.

Donné, etc.

Ainsi délibéré et adopté, en séance du Conseil d'Etat, à Lausanne, le 5 avril 2006.

Le président :	Le chancelier :
P. Broulis	*V. Grandjean*

Texte actuel

Champ dâpplication

Art. 2.- La présente loi s'applique aux autorités suivantes :

a. au Grand Conseil ;

b. au Conseil d'Etat et à son administration, à l'exclusion de ses fonctions juridictionnelles ;

c. à l'Ordre judiciaire et à son administration, à l'exclusion de ses fonctions juridictionnelles ;

d. aux autorités communales et à leurs administration, à l'exclusion de leurs fonctions juridictionnelles ;

Le Conseil d'Etat désigne les personnes morales et autres organismes de droit privé ou public assujettis à la présente loi. Ces derniers ne sont assujettis que lorsque et dans le mesure où ils agissent dans l'accomplissement de tâches de droit public. Le Conseil d'Etat précise l'étendue et les modalités de cet assujettissement**.**

Projet

PROJET DE LOI

modifiant la loi du 24 septembre 2002 sur l'information (LInfo)

LE GRAND CONSEIL DU CANTON DE VAUD

vu le projet de loi présenté par le Conseil d'Etat

décrète

***Article premier.* –** La loi du 24 septembre 2002 sur l'information est modifiée comme il suit :

Champ d'application

Art. 2.- La présente loi s'applique aux autorités suivantes :

a. au Grand Conseil ;

b. au Conseil d'Etat et à son administration, à l'exclusion de ses fonctions juridictionnelles ;

c. à l'Ordre judiciaire et à son administration, à l'exclusion de ses fonctions juridictionnelles ;

d. aux autorités communales et à leurs administration, à l'exclusion de leurs fonctions juridictionnelles ;

e. (nouveau) aux personnes physiques et morales auxquelles le canton ou une commune confie des tâches publiques.

(al. 2 supprimé)

	Texte actuel		Projet
	Art. 20 Pour toute demande du public portant sur des renseignements, la consultation de dossier ou sur une activité de l'administration cantonale, l'entité administrative compétente doit indiquer par écrit les motifs l'ayant conduite à ne pas donner son autorisation, à la donner partiellement ou à différer sa transmission.		**Art. 20** Pour toute demande fondée sur la présente loi, l'entité compétente doit indiquer par écrit les motifs l'ayant conduite à ne pas donner son autorisation, à la donner partiellement ou à différer sa transmission. **(al. 2 nouveau)** L'entité compétente adresse une copie de sa détermination au Préposé.
Médiation et recours	**Art. 21.-** L'entité compétente transmet sa détermination à l'intéressé qui peut saisir une le Préposé à la protection des données et à l'information, ou recourir directement au Tribunal administratif dans un délai de vingt jours dès la notification de la détermination. Passé ce délai, la détermination devient définitive. Si une procédure de médiation est ouverte, mais qu'elle n'aboutit pas à un accord qui satisfait les deux parties, la commission restreinte prend position sur l'affaire et donne ses recommandations écrites à l'entité et à l'intéressé. Ce dernier dispose alors d'un délai de vingt jours dès sa notification des recommandations de la commission pour recourir au Tribunal administratif. Cette procédure est également applicable aux personnes morales et autres organismes privés de droit public prévus à l'article 2, alinéa 2 de la présente loi.	**Saisine du Préposé**	**Art. 21. – (al. 1 nouveau)** L'intéressé peut saisir le Préposé par une demande en médiation sommairement motivée, dans un délai de vingt jours dès la notification de la détermination. Passé ce délai, la détermination devient définitive. (al. 2 et 3 supprimés)
		Médiation	**Art. 21 bis. –** Dès qu'il est saisi d'une demande en médiation, le Préposé la notifie à l'entité compétente. Le Préposé s'efforce d'amener les parties à un accord. Il dispose à cet effet des moyens décrits à l'article 41 de la loi sur la protection des données. Si la médiation aboutit, l'affaire est classée. Si une procédure de médiation n'aboutit pas à un accord qui satisfait les deux parties, le Préposé prend position sur l'affaire et donne sa recommandation écrite à l'entité compétente et à l'intéressé.

Texte actuel	Projet
	Décision **Art. 21 ter.** – L'entité compétente rend une décision dans les dix jours à compter de la date de réception de la recommandation. Elle notifie sa décision à l'intéressé et au Préposé.
	Gratuité **Art. 21 quater.** – La procédure est gratuite. Un émolument peut être perçu en cas de demande abusive. Le Conseil d'Etat fixe le tarif des émoluments.
	Recours **Art. 21 qinquies** – La décision de l'entité compétente est sujette à recours au Tribunal administratif. Le refus de statuer ou le dépassement du délai prescrit à l'article 34 alinéa 3 sont assimilés à une décision. La procédure de recours est régie par la loi sur loi sur la juridiction et la procédure administratives (RSV 173.36).
	Chapitre VI bis Préposé à la protection des données et à l'information
	Surveillance **Art. 27 bis .-** Le Préposé est chargée de : a) conduire la procédure de médiation et formuler une recommandation (article 21) lorsque la médiation n'aboutit pas ; b) informer, d'office ou à la demande de particuliers ou d'entités, des modalités d'accès à des documents officiels.
	Moyens **Art. 27 ter .-** Le Préposé dispose, dans le cadre de la médiation prévue à l'article 21, d'un droit d'accès aux documents officiels, même si ceux-ci sont tenus secrets
	***Art. 2.* –** Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale et en fixera, par voie d'arrêté, la date d'entrée en vigueur.

Texte actuel	Projet
	Donné, etc.
	Ainsi délibéré et adopté, en séance du Conseil d'Etat, à Lausanne, le 5 avril 2006.
	Le président : Le chancelier :
	P. Broulis *V. Grandjean*

Texte actuel

Projet

PROJET DE LOI

modifiant la loi du 15 septembre 1999 sur la statistique cantonale (LStat)

LE GRAND CONSEIL DU CANTON DE VAUD

LE GRAND CONSEIL DU CANTON DE VAUD

vu le projet de loi présenté par le Conseil d'Etat

décrète

Art. 19 bis nouveau. – Pour exécuter ses tâches statistiques, l'autorité compétente peut apparier des données à condition de les rendre anonymes. Si des données sensibles sont appariées ou si l'appariement de données permet d'établir des profils de la personnalité, les données appariées doivent être effacées une fois les travaux statistiques d'exploitation terminés

***Art. 2.* –** Le Conseil d'Etat est chargé de l'exécution de la présente loi. Il en publiera le texte conformément à l'article 84, alinéa 1, lettre a) de la Constitution cantonale et en fixera, par voie d'arrêté, la date d'entrée en vigueur.

Donné, etc.

Ainsi délibéré et adopté, en séance du Conseil d'Etat, à Lausanne, le 5 avril 2006.

Le président : Le chancelier :

P.. Broulis *V. Grandjean*