# Tableau de présentation de l'avant-projet de loi cantonale sur la protection des données personnelles

## Lexique

- Constitution fédérale, Cst.
- Constitution cantonale, Cst-VD
- Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel, Convention 108+
- Directive (UE) 2016/680 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, directive (UE) 2016/680
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), règlement (UE) 2016/679 (RGPD)
- Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE 223
- Loi fédérale du 25 septembre 2020 sur la protection des données, LPD
- Ordonnance du 31 août 2022 sur la protection des données, OPDo
- Loi du 11 septembre 2007 sur la protection des données personnelles, LPrD
- Rapport n°74 intitulé « Audit de la protection des données personnelles dans l'Administration cantonale vaudoise », rapport n°74 de la Cour des comptes
- Autorité : autorité de protection des données et de droit à l'information
- Préposé : Préposé à la protection des données personnelles du Canton de Vaud

| Commentaire | Remarques (consultation) |
|---|---|
| **Chapitre I But, champ d'application et organisation** | |

# Commentaire, article par article, de l'avant-projet de loi sur la protection des données personnelles

| Commentaire | Remarques (consultation) |
|---|---|
| **Art. 1 But**<br><br>Aucun changement substantiel n'est à relever. Le but de la loi reste la concrétisation du droit fondamental au respect de la sphère privée, garanti autant par la Constitution du Canton de Vaud (art. 15 Cst-VD) que par la Constitution fédérale (art. 13 Cst.). Dans ces deux textes, le droit d'être protégé contre l'utilisation abusive de ses données personnelles est explicitement mentionné. | *Avis général : favorable, avec une observation concernant les personnes morales.*<br><br>Contrairement à la LPD, le pLPrD confirme son application aux informations relatives aux personnes morales, qui sont également considérées comme des données personnelles conformément à la définition qui en est donnée à l'art. 5 al. 1 let. a pLPrD.<br><br>Bien que cela puisse donner l'impression d'une différence de régime entre la LPD et la LPrD, cette image est tempérée par le fait que le droit fédéral (aux art. 57r ss LOGA) prévoit aussi un régime spécifique au traitement de données concernant des personnes morales. L'on devrait toutefois plutôt concrétiser les règles de protection des données de personnes morales dans une partie distincte du pLPrD et non pas en « mélangeant » les règles sans distinction claire entre données de personnes morales et données personnelles de personnes physiques. |
| **Art. 2 Champ d'application**<br><br>Le champ d'application *ratione personae* de la loi reste fondamentalement inchangé. Le premier alinéa liste exhaustivement les entités soumises à la LPrD tandis que le second alinéa prévoit différentes exceptions. Ce sont donc essentiellement les entités publiques et parapubliques cantonales qui sont soumises à la législation cantonale en matière de protection des données personnelles. Cela comprend ainsi les autorités cantonales relevant des trois pouvoirs de l'Etat qui sont énumérées aux articles 89 à 136d de la Constitution cantonale (art. 2 al. 1 let. a pLPrD). Sont ainsi concernés au premier titre le Conseil d'Etat et l'ensemble de son administration dans ses subdivisions multiples (Chancellerie, départements, secrétariats généraux, directions générales, services, offices, bureaux, etc.), le Grand Conseil, son administration (Secrétariat général du Grand Conseil) et ses subdivisions (bureau du Grand Conseil, commissions parlementaires) ainsi que l'ordre judiciaire dans son ensemble, qu'il s'agisse des différents tribunaux ou du secrétariat général de l'ordre judiciaire. À noter que les autorités administratives indépendantes du | *Avis général : favorable, avec une demande d'ajout d'une règle de coordination entre la LPrD et la LPD pour les personnes privées auxquelles des entités cantonales ou communales confient une tâche publique et plusieurs remarques.*<br><br>S'agissant spécifiquement de l'application du pLPrD aux personnes physiques ou morales auxquelles les entités mentionnées aux lettres a à d confient une tâche publique, dans l'exécution de cette tâche, il serait utile de prévoir une règle de coordination avec le droit fédéral (auquel ces personnes sont, en principe, soumises pour leurs autres traitements), par exemple |

| Commentaire | Remarques (consultation) |
|---|---|
| Conseil d'Etat seront également soumises à la LPrD (cf. art. 2 al. 1 let. c pLPrD). On pensera ici notamment à la Cour des comptes, au Contrôle cantonal des finances, à l'Autorité de protection des données et de droit à l'information ou bien encore au Bureau cantonal de médiation administrative.<br>Les autorités communales et intercommunales seront également toutes assujetties à la LPrD (art. 2 al. 1 let. b pLPrD). Sont donc ici visées les autorités communales telles que définies par la loi du 28 février 1956 sur les communes ou certaines lois spéciales (p. ex : les commissions communales de recours en matière d'impôts au sens de la loi du 5 décembre 1956 sur les impôts communaux) ainsi que les fractions de communes et les différentes formes de collaborations intercommunales définies par la constitution et la loi.<br>Le champ d'application de la loi s'étend également aux personnes morales de droit public ainsi qu'à toute autre entité autonome, cantonale ou communale, créée par la loi (art. 2 al. 1 let. e pLPrD). Il s'agit donc d'entités publiques dont le statut, l'autonomie et les missions sont fixées par une loi cantonale ou un règlement communal. Sont ici à citer à titre d'exemples l'Université de Lausanne, l'Etablissement d'assurance contre l'incendie et les éléments naturels du Canton de Vaud (ECA), la Banque cantonale vaudoise (BCV), l'Association vaudoise d'aide et de soins à domicile (AVASAD), etc. Les Eglises reconnues de droit public – à savoir l'Eglise évangélique réformée du canton de Vaud (EERV) et la Fédération ecclésiastique catholique romaine du canton de Vaud (FEDEC-VD) pourraient dans une large mesure être rangées dans cette catégorie mais font toutefois l'objet d'une disposition particulière (art. 2 al. 1 let. f pLPrD), pour la bonne clarté, puisque leur existence juridique n'est pas créée mais simplement reconnue par la loi. Les communautés religieuses reconnues d'intérêt public ne sont en revanche pas des personnes morales de droit public. Vu leur statut de droit privé, elles sont soumises à la LPD, non à la LPrD.<br>Comme dans la loi actuelle, les personnes physiques et morales auxquelles le canton, les communes ou les personnes morales de droit public confient des tâches publiques seront soumises à la LPrD, étant entendu que cette soumission ne s'étend qu'à l'exécution des tâches publiques confiées.<br>Le second alinéa prévoit l'exclusion de certaines matières du champ d'application de la LPrD, quand bien même le responsable du traitement est soumis à la loi en vertu du premier alinéa :<br>- L'inapplicabilité de la loi aux délibérations du Grand Conseil et des conseils généraux et communaux est une reprise de la loi actuelle ;<br>- La LPrD ne s'applique ni aux procédures civiles et pénales ni aux procédures administratives contentieuses. Les lois de procédure topiques (principalement : le code de procédure civile, le code de procédure pénale, la loi vaudoise sur la procédure administrative) s'appliquent donc exclusivement, ceci afin d'éviter les collisions de normes entre les lois précitées et la LPrD ;<br>- Les traitements de données des entités soumises à la LPrD qui relèvent d'activités soumises à la concurrence économique régie par le droit privé (et non de l'exécution de tâches publiques) n'entreront pas dans le champ d'application de la LPrD et seront soumises aux dispositions de la LPD applicables aux personnes privées. En vertu | en prévoyant l'application du régime le plus protecteur du droit de la protection des données en cas de divergence ou contradiction.<br><br>Il serait bienvenu de préciser dans le rapport s'il y a d'autres personne morale de droit public qui sont dans un rapport de concurrence, notamment s'agissant de l'Université de Lausanne, l'Etablissement d'assurance contre l'incendie et les éléments naturels du Canton de Vaud (ECA) et l'Association vaudoise d'aide et de soins à domicile (AVASAD), etc. |

| Commentaire | Remarques (consultation) |
|---|---|
| du principe d'égalité entre les concurrents, on ne saurait soumettre les acteurs du marché à deux régimes légaux distincts. Aussi la LPD fédérale s'appliquera de manière uniforme à tous les concurrents. Seront concernées dans le canton de Vaud, par exemple, les activités de la Banque cantonale vaudoise. Bien qu'il s'agisse d'une personne morale de droit public créée par une loi, les activités de la BCV s'inscrivent pour l'essentiel dans un rapport de concurrence économique relevant du droit privé. L'ensemble des activités concernées sera donc uniquement soumis à la loi fédérale sur la protection des données, comme le sont les organismes bancaires au bénéfice d'un statut de droit privé. Il ne pourra toutefois s'agir d'une application directe de la LPD. En effet, cette législation restreint son champ d'application personnel aux personnes privées et aux organes fédéraux (art. 2 al. 1 LPD). Les personnes morales de droit public relevant du droit cantonal n'y sont donc pas directement soumises. Il convient dès lors de préciser dans la LPrD que l'application des dispositions relatives aux personnes privées de la loi fédérale est une application par analogie. En outre, un corollaire de ce qui précède est l'absence de compétence du Préposé fédéral à la protection des données et à la transparence (PFPDT) d'exercer une quelconque surveillance sur les personnes morales de droit public cantonal ; sa mission se limite à surveiller les personnes et autorités visées par la LPD. Un tel vide juridique doit être comblé de sorte qu'une surveillance des traitements de données effectués par des personnes morales de droit public cantonal engagées dans un rapport de concurrence économique puisse être exercée par une autorité indépendante. Le Conseil d'Etat propose en conséquence d'étendre les compétences de l'autorité de protection des données et de droit à l'information. Il lui incombera de surveiller la correcte application des prescriptions fédérales en matière de protection des données applicables aux personnes privées par les personnes morales de droit public cantonal exerçant une activité de droit privé soumise à la concurrence économique. Pour ce faire, l'autorité bénéficiera des pouvoirs d'enquête et de décision qui lui sont conférés par les art. 39 à 42 pLPrD. Ces prérogatives sont similaires à celles dont dispose le PFPDT (cf. art. 49 à 52 LPD). » | |
| **Art. 3 Autorité de protection des données et de droit à l'information**<br><br>L'article 3 est une disposition générale qui institue l'Autorité de protection des données et de droit à l'information (ci-après : l'Autorité) et fixe la ligne d'ensemble de son mandat, à savoir de surveiller la bonne application des prescriptions de la LPrD et de la LInfo. Les prérogatives de l'autorité en matière de surveillance sont définies exhaustivement au chapitre V pLPrD.<br>Sur le modèle suivi par la Confédération, le Conseil d'Etat propose d'exclure le Grand Conseil, le Conseil d'Etat et le Tribunal cantonal du spectre de la surveillance exercée par l'Autorité. En effet, une telle surveillance serait susceptible de nuire à la séparation des pouvoirs et à l'indépendance de la justice. Pour ce qui est des autres entités exerçant des fonctions juridictionnelles comme les tribunaux inférieurs au Tribunal cantonal, le Ministère public ou certaines autorités communales comme les commissions de recours en matière d'impôts, il convient de rappeler l'inapplicabilité de la LPrD et l'application exclusive des règles de procédure topiques. Dès lors que la LPrD n'est | *Avis général : favorable, avec une demande d'analyse et de précision quant au choix du Conseil d'Etat et plusieurs remarques.*<br><br>Le système proposé, qui prévoit une autorité commune à la protection des données et à l'information tout en assurant la nature bicéphale de sa direction (deux préposés ou préposées), reprend le système actuellement appliqué. Il serait toutefois intéressant de savoir pourquoi le Conseil d'Etat n'a pas retenu une solution intégrant deux autorités de protection des données distinctes, soit (i) un ou une préposé ou préposée, et (ii) une commission en |

| Commentaire | Remarques (consultation) |
|---|---|
| pas applicable dans les procédures civiles, pénales ou administratives contentieuses, la surveillance de l'Autorité ne saurait s'étendre à ces dernières. En revanche, des mesures de surveillance sont envisageables pour les activités non-juridictionnelles des entités précitées.<br>L'organisation bicéphale de l'Autorité, aujourd'hui une réalité dans la pratique, trouve désormais une concrétisation dans la loi (art. 3 al. 3 pLPrD). La personne qui dirige l'Autorité, appelée Préposé ou Préposée à la protection des données, sera désignée par le Conseil d'Etat et aura pour mission principale de contrôler la bonne application des dispositions de la LPrD. Le Conseil d'Etat nommera également une personne Préposé ou Préposée au droit à l'information (cf. chapitre V pLPrD) et celle-ci sera chargée de traiter les demandes relevant de la Loi du … sur l'information (LInfo). | matière de protection des données, à l'image de ce qui se retrouve dans d'autres cantons (p.ex. Valais. Jura, Neuchâtel ou Fribourg). Une telle solution à deux autorités, bien que n'étant pas toujours nécessaire, présente plusieurs avantages en comparaison à un système d'autorité unique, notamment pour ce qui est de la répartition de la charge de travail ainsi que le travail avec les communes. Compte tenu des problématiques qui sont apparues ces dernières années au sein de plusieurs communes vaudoises quant au respect des règles en matière de protection des données, il serait intéressant d'au-moins étudier la possibilité de créer aussi une commission cantonale.<br><br>A notre sens et sur la base des éléments actuels, il serait préférable de choisir un modèle largement partagé dans les cantons latins avec un Préposé qui conseille, surveille, concilie et instruit, et émet des recommandations, et une autorité ou commission qui rend des décisions. Voir à ce sujet également les commentaires ad art. 40 ss infra.<br><br>Cette disposition devrait figurer dans le chapitre V. Elle mélange la composition de l'Autorité et ses compétences.<br><br>Rien ne justifie l'exclusion de l'al. 2 (dans la mesure où la LPrD est applicable). |
| **Art. 4 Personnes de référence en matière de protection des données** | *Avis général : favorable, avec une demande de modification terminologique et un ajout.* |

# Commentaire, article par article, de l'avant-projet de loi sur la protection des données personnelles

| Commentaire | Remarques (consultation) |
|---|---|
| Dans son rapport n°74 intitulé « Audit de la protection des données personnelles dans l'Administration cantonale vaudoise » (rapport n°74 de la Cour des comptes), la Cour des comptes recommandait au Conseil d'Etat de désigner un délégué à la protection des données dans chaque entité-métier. Le Conseil d'Etat propose ainsi de donner suite à cette recommandation par l'obligation faite à chaque département de désigner au minimum une personne spécialiste de la protection des données qui aura pour tâche principale de conseiller et d'informer les responsables du traitement ainsi que les collaborateurs des différents services du département (art. 4 al. 1 pLPrD). Il fera également office de point de contact avec l'Autorité (cf. art. 4 al. 3 LPrD). Il lui incombera également de proposer des mesures lorsqu'il apparaîtra que des prescriptions relatives à la protection des données ont été violées. Cette personne devra bien entendu bénéficier des connaissances professionnelles nécessaires, attestées par une formation qualifiante ou une expérience professionnelle pertinente. L'indépendance de la personne nommée dans l'accomplissement de ses tâches en matière de protection des données est en outre garantie par la loi (cf. art. 4 al. 3 pLPrD).<br>Quant à l'alinéa 3, il vise à ancrer dans le droit cantonal l'obligation prescrite à l'article 32 de la directive (UE) 2016/80 (directive Schengen) qui prévoit la nomination d'un conseiller à la protection des données par chaque responsable du traitement actif dans le domaine couvert par la directive précitée, soit les domaines de la police et de la justice pénale. La nomination d'un conseiller commun à plusieurs responsables de traitement est possible. L'art. 4 al. 2 PLPrD a pour but de remplacer l'art. 10 LPrDS qui sera abrogé au moment de l'entrée en vigueur de la LPrD. | Alors que le titre de l'article se réfère aux « personnes de référence en matière de protection des données », les al. 2 et 3 utilisent tous deux le terme de « conseiller à la protection des données » et de spécialiste de la protection des données. Or, ce terme ne vise pas, dans les deux cas, le même type de rôle et de personne. En effet, l'al. 2 prévoit un « conseiller à la protection des données » dans les départements, alors que l'al. 3 couvre le référent UE (qui est, donc, également désigné ici comme conseiller à la protection des données). Cet usage d'un même terme n'est pas clair – il faudrait donc clarifier la terminologie pour éviter une confusion entre ces deux personnes, qui ne sont pas les mêmes et n'ont pas directement la même fonction.<br><br>Cette disposition ne concerne que l'Etat de Vaud, à l'exclusion des communes. Pourtant, il est essentiel de s'assurer que celles-ci disposent également formellement d'une personne ayant des compétences en matière de protection des données, dans la mesure où plusieurs problématiques récentes dans ce domaine sont intervenues au niveau communal. En conséquence, la fonction de personne de référence en matière de protection des données doit être étendue aux communes et autres entités communales, avec toutefois la possibilité devant explicitement être prévue d'une mutualisation de cette fonction entre plusieurs communes ou entités communales, à l'image de ce qui se retrouve par exemple en droit valaisan (art. 30c LIPDA). |

| Commentaire | Remarques (consultation) |
|---|---|
| **Chapitre II Dispositions générales, principes** | |
| **Art. 5 Définition**<br><br>La liste des définitions des termes utilisés dans la loi a subi quelques ajustements.<br>La principale modification tient dans l'extension des catégories des données personnelles sensibles. Par comparaison aux catégories actuelles, on relèvera donc l'ajout des données génétiques ainsi que des données biométriques identifiant une personne physique de manière univoque. Il s'agit, là encore, de se conformer au droit supérieur, en particulier l'art. 6 par. 1 de la convention 108+ et l'art. 10 de la directive (UE) 2016/680 ainsi que l'art. 5 let. c LPD. A cet égard, les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN (au sens de l'art. 3 let. l de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine). Par données biométriques, il convient d'entendre les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel n'est, en principe, pas le cas, par exemple, de simples photographies.<br>La notion de « profil de la personnalité » est abandonnée au profit de celle de « profilage ». Le canton s'aligne sur la solution retenue par la Confédération. Comme l'explique le Conseil fédéral dans son message explicatif relatif à la nouvelle loi fédérale sur la protection des données, le terme de « profil de la personnalité » était une spécificité de la législation suisse, qui n'existe pas en droit européen et qui n'est pas connu des législations étrangères. En revanche, la notion de « profilage » est connue en droit européen, puisqu'on la retrouve à l'art. 3 par. 4 de la directive (UE) 2016/680 et à l'art. 4 par. 4 du règlement (UE) 2016/679.<br>Les deux notions, bien que présentant plusieurs similitudes, ne couvrent pas le même état de fait. Le profil de la personnalité est le résultat d'un traitement et traduit ainsi quelque chose de statique. À l'inverse, le profilage désigne une forme particulière de traitement, et constitue donc un processus dynamique, caractérisé par le traitement de données de manière automatisée.<br>Ainsi, comme le précise le Conseil fédéral dans son message, le profilage est défini comme l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, afin notamment d'analyser ou de prédire son rendement au travail, sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements. L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité. Autrement dit, le profilage se | *Avis général : favorable, avec deux observations.*<br><br>Cf. commentaire *ad* art. 1 pour l'intégration des personnes morales en tant que personnes concernées, respectivement pour l'extension de la définition des données personnelles aux informations qui se rapportent à une personne morale.<br><br>Il est positif que le pLPrD ne reprenne pas la distinction entre « profilage » et « profilage à risque élevé » qui avait été introduite par le Parlement fédéral dans la LPD. Cette distinction crée en effet des risques d'interprétation en pratique et rend les notions utilisées peu claires. En outre, elle ne se justifie dans tous les cas pas dans une loi – telle que le pLPrD – qui cible le traitement de données personnelles effectuées principalement par des entités publiques.<br><br>Let. h. le rapport pourrait donner des exemples de qui est le responsable du traitement vu l'incertitude qui existe au sein de l'administration (département, service, etc.) et des communes (un seul responsable du traitement ou chaque service communal).<br><br>Let i. on voit mal à quel organisme il est fait référence (qui ne serait ni une personne ni une autorité publique). |

| Commentaire | Remarques (consultation) |
|---|---|
| caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé. On entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible mais non constitutif du profilage. En revanche, l'évaluation automatisée des données est indispensable. La simple accumulation de données n'est pas assimilée au profilage. L'évaluation automatisée vise en particulier à analyser ou à prédire certains comportements de la personne. La loi cite quelques exemples de caractéristiques personnelles, telles que le rendement au travail, la situation économique ou la santé. On peut en imaginer d'autres, comme la fiabilité ou le lieu de résidence.<br>La disparition de la notion de « fichier » au profit de celle de « registre des activités de traitement ». La notion de « fichier » a en effet été supprimé tant du droit européen – la Convention 108+ n'y fait plus référence et parle désormais de traitement – que du droit fédéral. À ce propos, le registre des activités de traitement est défini comme un répertoire en ligne inventoriant les activités de traitement réalisées par les responsables du traitement soumis à la LPrD. Le registre des activités de traitement contient en principe les indications suivantes : le nom du responsable du traitement; la finalité du traitement; une description des catégories des personnes concernées et des catégories des données personnelles traitées; les catégories des destinataires; la durée de conservation des données personnelles ou, si cela n'est pas possible, les critères pour déterminer la durée de conservation; dans la mesure du possible, une description générale des mesures visant à garantir la sécurité des données; l'Etat tiers ou l'organisme international auquel des données personnelles sont communiquées ainsi que les garanties de protection des données personnelles prévues.<br>Enfin, il convient de relever de la suppression des notions de « procédure d'appel », de « loi au sens formel » et de « vidéosurveillance dissuasive ». La procédure d'appel étant un mode de communication des données, elle peut être subsumée sous cette catégorie plus générale. La notion de « loi au sens formel » est une catégorie générale du droit public et sa définition est superflue dans une loi dédiée à la protection des données personnelles ; la Confédération l'a également supprimée de la LPD pour ce motif. Quant au terme de « vidéosurveillance dissuasive », il sera dorénavant défini dans la loi spécifiquement consacrée à la vidéosurveillance. À cet égard, le Conseil d'Etat se permet de renvoyer au commentaire de l'art. 2 pLVidéo. | Let. l on voit mal pourquoi les autorités sont exclues. Il faudrait aussi uniformiser la mention de la nature de droit privé ou publique des personnes morales. |
| **Art. 6 Légalité**<br><br>En vertu du principe de la légalité inscrit à l'art. 5 al. 1 Cst-VD, toute action de l'Etat – comme le traitement ou la communication de données personnelles – nécessite une base légale. Lorsqu'il s'agit de porter atteinte à des droits fondamentaux comme la protection de la sphère privée, l'exigence quant au rang de la base légale et son degré de densité normative varie en fonction de la gravité de l'atteinte. Ainsi une atteinte grave exigera d'être prévue dans | |

| Commentaire | Remarques (consultation) |
|---|---|
| une loi au sens formel tandis qu'une atteinte d'une portée plus faible pourra être envisagée dans une loi au sens matériel.<br>L'art. 6 pLPrD a ainsi été rédigé dans cet esprit de gradation du principe de la légalité, en reprenant pour l'essentiel la disposition actuelle (art. 5 LPrD).<br>Les entités soumises à la loi pourront ainsi traiter des données personnelles non-sensibles à condition qu'une base légale l'autorise, celle-ci pouvant être une base légale matérielle comme un règlement du Conseil d'Etat. Alternativement, le traitement de données non-sensibles sera également licite si l'accomplissement d'une tâche légale l'exige. À cet égard, il conviendra qu'il existe un rapport raisonnable entre les données traitées et la tâche légale à accomplir, en ceci que l'on ne saurait concevoir, en suivant les règles de la bonne foi, que l'entité concernée puisse exécuter ses missions sans traiter les données personnelles concernées.<br>Dès lors qu'un traitement de données sensibles ou un profilage sont susceptibles de constituer, selon la jurisprudence, une atteinte grave aux droits fondamentaux des personnes concernées, il doit être expressément prévu dans une loi au sens formel, à savoir une loi adoptée par le Grand Conseil ou, au niveau communal, un règlement adopté par le Conseil général ou communal. La licéité d'un traitement de données sensibles ou d'un profilage devra également être admise lorsque l'accomplissement d'une tâche clairement définie dans une loi au sens formel l'exige absolument. Afin de ne pas vider le principe de la légalité de sa substance, une interprétation stricte sera de mise. Pour que le traitement de données n'ait pas à être expressément prévu dans une loi au sens formel, il faudra qu'il apparaisse comme une condition *sine qua non* de l'accomplissement de la tâche légale du service, traitement sans lequel l'activité du service pourrait être paralysée.<br>L'art. 6 al. 3 pLPrD prévoit une dérogation à l'exigence d'une base légale pour le traitement de données personnelles, y compris sensibles ou la réalisation de profilages. Pour que cette dérogation s'applique, il faut que l'une des deux conditions suivantes soit réalisée :<br>- Le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable. Cette dérogation est une transposition de l'art. 34 al. 4 let.c LPD et correspond à l'art. 10 let. b de la directive (UE) 2016/680 et à l'art. 6 par. 1 let. d du règlement (UE) 2016/679 ;<br>- La personne concernée a consenti au traitement en l'espèce ou a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. Cette dérogation est largement reprise du droit actuel et se retrouve également dans le droit fédéral (cf.art. 34 al. 4 let. c LPD).<br>Enfin, l'art. 6 al. 4 LPrD réserve le dispositif légal particulier qui permet au Conseil d'Etat d'autoriser des essais pilotes, au sens de l'art. 23 LPrD. | |
| **Art. 7 Finalité** | |

| Commentaire | Remarques (consultation) |
|---|---|
| L'alinéa 1 est repris tel quel de la législation en vigueur (art. 6 al. 1 LPrD).<br>Le second alinéa vise à élargir quelque peu la portée du principe de finalité en permettant aux entités soumises à la LPrD de traiter des données personnelles au-delà du but indiqué lors de la collecte si, selon les règles de la bonne foi, ce traitement ultérieur apparaît compatible avec le but initial. À titre d'exemple, on pourra citer le cas d'un service ayant récolté les adresses courriel des administrées en vue de leur communiquer une information et qui utilisent ces adresses afin de transmettre aux personnes concernées des informations qui pourraient les intéresser.<br>Le consentement de la personne concernée au changement de finalité du traitement de ses données personnelles est également explicitement prévu par le projet de loi. | |
| **Art. 8 Proportionnalité**<br><br>**Art. 9 Transparence**<br><br>Ces dispositions n'ont pas été modifiées. | *Avis général : favorable, avec une observation.*<br><br>Il serait utile de préciser dans le commentaire ce que le principe de transparence implique réellement, en particulier vu que l'obligation d'informer a été fortement réduite par rapport à la LPrD actuelle. |
| **Art. 10 Exactitude**<br><br>Sur le fond, le principe d'exactitude n'est pas nouveau. La disposition a toutefois été reformulée et étoffée de manière à correspondre au droit supérieur, notamment l'art. 6 al. 5 LPD.<br>Le texte prévoit que le responsable du traitement doit s'assurer que les données personnelles traitées sont exactes. Il lui incombe donc de prendre toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. En conséquence, les données qui ne peuvent être rectifiées ou complétées doivent être effacées ou détruites. L'étendue du devoir d'exactitude doit être déterminée de cas en cas. Elle dépend notamment de la finalité du traitement ainsi que de son ampleur, et du type de données traitées. Le devoir d'exactitude peut impliquer selon les cas de tenir les données à jour.<br>Le principe d'exactitude ne saurait s'appliquer de manière absolue et doit souffrir quelques aménagements. Ainsi, dans certains cas, certaines obligations et principes légaux peuvent s'opposer à la rectification, à l'effacement, ou à la mise à jour des données. Le principe d'exactitude et les devoirs qui y sont liés doivent par ailleurs être aménagés de manière différenciée pour les archives, les musées, les bibliothèques et les autres institutions patrimoniales publiques, de sorte que la rectification, l'effacement ou la mise à jour des données ne doit pas avoir lieu dans certains cas. Les tâches de ces institutions consistent notamment à collectionner, à répertorier, à conserver et à rendre accessible des documents – numériques ou non – de toutes sortes. Ces documents ne doivent en eux-mêmes | *Avis général : favorable, avec une observation*<br><br>Les réserves relatives notamment aux activités d'archivage ou aux données présentant une importante patrimoniale, qui figurent dans les explications ci-contre, devraient être reprises dans la disposition de façon résumée. |

| Commentaire | Remarques (consultation) |
|---|---|
| pas être modifiés, car cela irait à l'encontre du but même de l'archivage. Les archives doivent, grâce à ces documents, permettre d'avoir une photo du passé à un moment donné. Leur exactitude se réfère ainsi uniquement à la question de savoir si les documents en question ont été reproduits fidèlement. En d'autres termes, les archives rendent état d'une situation dans le passé, et cela indépendamment du fait de savoir si cette dernière est exacte selon une perspective actuelle. Il existe un intérêt public prépondérant pour cette activité particulière. | |
| **Art. 11 Sécurité**<br><br>La disposition consacrée à la sécurité des données est calquée sur le texte de l'art. 8 LPD. Le devoir d'assurer la sécurité des données est une exigence de la Convention 108+ (art. 7) et de la directive (UE) 2016/680 (art. 29). Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Cette disposition matérialise l'approche fondée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées.<br>L'alinéa 2 mentionne le but des mesures. Ces dernières doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite.<br>L'alinéa 3 permet au Conseil d'Etat de définir des exigences minimales en matière de sécurité des données personnelles. | *Avis général : favorable, avec un complément.*<br><br>Compte tenu des risques toujours plus marqués en termes de sécurité des données, il est impératif d'avoir une disposition plus précise dans la loi, laquelle est ensuite appelée à être détaillée dans le Règlement. Un tel régime existe notamment dans la LIPDA valaisanne (art. 21). Il conviendrait ainsi notamment de prévoir directement dans la loi que les mesures organisationnelles et techniques appropriées comprennent notamment :<br>- la pseudonymisation et le chiffrement des données personnelles ;<br>- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; et<br>- des moyens permettant de rétablir la disponibilité des données personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique.<br><br>La nécessité de procéder à un examen périodique des mesures mises en œuvre, et cas échéant à leur adaptation, devrait aussi explicitement être prévue dans la loi. |
| **Art. 12 Consentement** | |

| Commentaire | Remarques (consultation) |
|---|---|
| Le consentement de la personne concernée au traitement de ses données personnelles revêt une importance moindre dans le secteur public que dans le secteur privé. En effet, le fondement permettant aux organes de l'Etat, personnes morales de droit public et autres entités parapubliques de traiter des données personnelles réside, dans la majeure partie des cas, dans la loi et non dans le consentement des personnes concernées. Le consentement peut toutefois être requis dans certains cas de figure, par exemple à titre de dérogation du principe de la légalité (cf. art. 6 al. 3 let. b pLPrD) ou pour le changement de finalité d'un traitement de données (cf. art. 7 al. 2 pLPrD).<br>Ce préalable étant posé, la disposition consacrée au consentement n'a fait l'objet que d'une précision terminologique dans sa seconde phrase. Aussi lorsqu'il s'agira de traiter des données sensibles ou de procéder à un profilage, le consentement de la personne concernée ne sera valable que s'il satisfait aux exigences – inchangées en comparaison du droit actuel – formulées dans la première phrase et qu'il est au surplus *exprès,* notion qui remplacera celle de l'actuel art. 12 LPrD, lequel parle de consentement *explicite*. Ce changement de terme permet de s'aligner sur le droit fédéral (cf. art. 6 al. 7 LPD) et, d'autre part, d'employer un terme juridique plus courant, notamment en droit privé, que le mot « explicite ». On rappellera qu'une déclaration de volonté est « expresse » lorsqu'elle est formulée oralement, par écrit ou par un signe, et qu'elle découle directement des mots employés ou du signe en question. En ceci, un consentement exprès s'oppose un consentement simplement *tacite*. Une déclaration de volonté en tant que telle doit, dans sa forme même, permettre à la personne concernée de reconnaitre clairement qu'elle est en train de manifester sa volonté. Dans le domaine informatique, l'exigence du consentement exprès est ainsi satisfaite lorsqu'une case invitant la personne concernée à consentir au traitement de ses données est cochée.<br>Pour le reste, la portée de la disposition demeure inchangée. | |
| **Art. 13 Protection des données dès la conception et par défaut**<br><br>La double exigence d'assurer la protection des données dès la conception et par défaut est une disposition nouvelle découlant du droit supérieur. L'art. 13 pLPrD est ainsi une transposition de l'art. 7 LPD. Une telle disposition permet de mettre le droit cantonal en conformité aux exigences des art. 8bis par. 3 de la Convention 108+ et 20 par. 1 de la directive (UE) 2016/680.<br>L'alinéa 1 impose au responsable du traitement de concevoir dès l'origine le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. Cette obligation nouvelle repose sur le principe de la technologie au service de la protection des données personnelles (*privacy by design*). Comme l'explique le Conseil fédéral dans son message explicatif relatif à la LPD, le recours à des solutions techniques pour garantir la protection des données s'appuie sur l'idée que la technologie et le droit se complètent. Ainsi, des solutions techniques qui rendent impossible une violation de la protection des données ou qui en réduisent la probabilité rendent les règles juridiques et les codes de conduite moins nécessaires. Par ailleurs, ces technologies sont | *Avis général : favorable avec deux observations*<br><br>Il est positif de reprendre en droit vaudois les obligations de protection des données dès la conception et par défaut. Cela étant, et comme cela découle de la phrase précitée, il s'agit bien d'une *obligation* et non de *principes*. En conséquence, il serait nécessaire de déplacer l'art. 13 dans le Chapitre III.<br><br>Par ailleurs, vu la nature souvent peu précise et générale des principes découlant de ces deux obligations, il conviendrait de prévoir à l'art. 13 que l'Autorité publie des lignes directrices sur leur mise |

| Commentaire | Remarques (consultation) |
|---|---|
| indispensables pour mettre en œuvre les réglementations de protection des données. La protection technique des données personnelles ne s'appuie cependant pas sur une technologie précise ; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis à l'art. 11 pLPrD (sécurité des données). En d'autres termes, les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données sont déjà intégrées dans le système, de manière à rendre impossible une violation de la protection des données ou d'en réduire la probabilité. Il s'agit par exemple de la fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique des données personnelles. Un principe significatif pour la protection des données sur plan technique est celui de la minimisation des données, qui ressort aussi du principe de sécurité des données. Selon ce dernier, il faut fixer avant même le début d'un traitement ses modalités, de manière que le moins de données possible soient traitées, et de façon qu'elles soient conservées le moins longtemps possible.<br>L'al. 2 précise les exigences auxquelles doivent satisfaire les mesures visées à l'al. 1. Ces mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue et du degré de probabilité et de gravité du risque que le traitement des données personnelles en question présente pour la personnalité et les droits fondamentaux des personnes concernées. Une telle norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées.<br>Selon l'al. 3, le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement (*privacy by default*). Dans le contexte de la protection des données personnelles, cela signifie que le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données, mais qu'on laisse à la personne concernée la possibilité d'en modifier les paramètres. La protection des données personnelles par défaut permet en conséquence à la personne concernée de consentir à un traitement déterminé. En ce qu'il repose principalement sur le consentement de la personne concernée, la protection des données par défaut joue un rôle mineur dans le secteur public. En effet, les traitements y reposent moins sur le consentement de la personne concernée que sur des dispositions légales (cf. le commentaire de l'art. 12 pLPrD ci-dessus) qui définissent le spectre des données personnelles qui peuvent faire l'objet d'un traitement. | en œuvre concrète, notamment à l'attention des entités de taille modeste (petites communes, associations intercommunales, etc.), dans la partie conseil de ses compétences. |
| **Chapitre III Traitement de données personnelles** | |
| **Art. 14 Responsabilité** | |

| Commentaire | Remarques (consultation) |
|---|---|
| Ce nouvel article sur la responsabilité permet de mettre le droit cantonal en conformité aux exigences du droit supérieur telles qu'elles ressortent notamment de l'art. 21 de la directive (UE) 2016/680. Également fondé sur l'expérience pratique, le projet de loi propose de poser directement dans la LPrD des règles claires, s'agissant du cas dans lequel deux ou plusieurs responsables du traitement traitent conjointement de données personnelles. L'article 14 ancre ainsi le principe de la responsabilité conjointe des différents responsables.<br><br>Formellement, l'art. 5 al. 1 let. h définit qu'un ou plusieurs responsables peuvent déterminer la finalité et les moyens du traitement. Il en découle que, dès lors que plusieurs entités soumises à la présente loi interviennent dans un traitement de données, celui-ci doit être qualifié de conjoint. La responsabilité de l'un ou de l'autre responsable peut varier en fonction du rôle exercé et un même niveau d'implication n'est pas requis pour que les responsables soient considérés comme conjoints. Le traitement conjoint ne doit néanmoins pas être confondu ou assimilé à la sous-traitance qui elle répond à des règles spécifiques (cf. art. 21 ci-dessous et son commentaire). En effet, le rapport de sous-traitance implique que le sous-traitant n'a aucune marge décisionnelle sur la finalité et les moyens liés au traitement de données ; il intervient comme exécutant pour le compte du responsable du traitement.<br>Finalement, les droits de la personne concernée implique une vision claire de qui, entre les responsables conjoints, assume quoi. Ainsi la répartition des responsabilités respectives doit être compréhensible et accessible facilement. | |
| **Art. 15 Devoir d'informer lors de la collecte de données personnelles**<br><br>En préambule, il est important de souligner que cette disposition doit se lire en parallèle avec la suivante (cf. art. 16 al. 1 pLPrD) qui prévoit *les exceptions au devoir d'informer notamment si le traitement des données personnelles ressort de la loi*. Dès lors, comme les traitements de données par des entités visées à l'art. 2 al. 1 pLPrD devront en principe se fonder sur des bases légales (art. 6 al. 1 et 2 pLPrD, ainsi que 6 al. 3 let. c LPrD), au contraire de ceux que réalisent les personnes privées, l'application de l'art. 15 pLPrD restera très limitée.<br><br>Au surplus, la disposition sur le devoir d'informer lors de la collecte de données personnelles reprend en grande partie les règles du droit vaudois actuel, ainsi que le texte de l'art. 19 LPD.<br>L'alinéa 1 reprend le principe d'une information lors de chaque collecte de données personnelles mais précise que cette information doit se faire de manière adéquate et également lorsque la collecte est effectuée auprès de tiers. Les informations doivent être facilement accessibles, reconnaissables et compréhensibles ; il importe que la personne concernée puisse reconnaître le traitement et en comprendre la portée. Cependant, si le responsable du traitement doit veiller à ce que les informations soient accessibles, le choix de les consulter appartient bien à la personne concernée. S'agissant plus spécialement des traitements pour lesquels la collecte de données personnelles s'effectue auprès de tiers, le projet reprend les règles actuelles (cf. alinéa 4). | *Avis général : favorable avec deux remarques*<br><br>Art. 15 al. 2 let. d : il ne devrait pas être nécessaire de communiquer les catégories de données personnelles traitées lorsque les données sont collectées auprès de la personne concernée (cf. art. 19 al. 3 LPD).<br><br>L'al. 4 doit viser les informations des al. 2 et 3. |

| Commentaire | Remarques (consultation) |
|---|---|
| L'alinéa 2 propose de modifier, dans le respect des nouvelles exigences du droit supérieur, l'actuel art. 13 sur le *Devoir d'informer* en ce sens qu'il incombera désormais au responsable du traitement de rendre les informations disponibles en tout temps, et non simplement lorsque la personne concernée en fait la demande. Cette dernière doit pouvoir obtenir ces informations sans avoir à les demander. Par ailleurs l'un des buts poursuivis avec la révision étant de renforcer les droits de la personne concernée, l'al. 2 dresse une liste minimale des informations que la personne concernée doit avoir en sa possession dans l'hypothèse où elle souhaiterait faire valoir ses droits.<br>Si la liste des informations à fournir est étoffée de façon à garantir la transparence sur les catégories de données personnelles traitées et à renforcer les droits de la personne concernée, elle permet tout de même une mise en œuvre souple, en prévoyant que le degré de détail des informations à fournir dépend des caractéristiques et risques de chaque traitement.<br>L'alinéa 3 ajoute des aspects au devoir d'informer du responsable du traitement lorsque des données personnelles sont transmises à l'étranger. On vise ici le nom de l'Etat destinataire et, cas échéant, les exceptions au sens de l'art. 20 al. 2 (cf. commentaire ci-dessous) qui sont invoquées.<br>L'alinéa 4 fixe le délai maximum dans lequel le responsable du traitement doit informer la personne concernée de la collecte de ses données personnelles auprès d'un tiers. Les délais qui figurent ici sont calqués sur ceux de l'art. 17 al. 5 LPD. | |
| **Art. 16 Exceptions au devoir d'informer et restrictions**<br><br>L'art. 16 reprend remplace l'actuel art. 14 LPrD. Sa structure et sa rédaction correspondent pour bonne part à celles de l'art. 20 LPD.<br><br>L'alinéa 1 indique que le devoir d'informer selon l'article 15 LPrD ne s'applique pas lorsque le traitement de données ressort de la loi. Comme relevé dans le commentaire relatif à cet article 15 LPrD, concrètement, ceci représentera la grande majorité des situations. En effet, les traitements de données par des entités soumises à la LPrD seront très généralement fondés sur la loi (cf. art. 6 al. 1 et 2 et al. 3, let. c pLPrD). La légère différence de formulation entre l'art. 16 pLPrD et l'art. 20 LPD (qui mentionne que le traitement de données doit être « prévu par la loi ») s'explique par le fait que le présent projet prévoit que des traitements de données pourront être accomplis non seulement lorsqu'ils sont directement prévus par la loi (art. 6 al. 1 let. a et 6 al. 1 let. a pLPrD), mais aussi lorsqu'ils sont indispensables à la réalisation d'une tâche légale (art. 6 al. 1 let. b et 6 al. 2 let. b). Dans ce second cas, si, à la lecture de la loi prévoyant la tâche légale, on peut aisément comprendre les traitements de données qui seront réalisés pour l'accomplir (ce qu'exprime le terme « ressort »), il serait disproportionné et source de coûts inutiles d'exiger de l'administration qu'elle fournisse en plus une information spéciale. | *Avis général : défavorable*<br><br>L'art. 16 est un recul par rapport à l'art. 14 LPrD qui prévoit une exception à l'obligation d'informer lorsque la loi le prévoit expressément et non pas lorsque le traitement « ressort » de la loi, ce qui semble viser les cas de la base légale au sens de l'art. 6 al. 1. Avec la solution proposée, les entités n'informeraient presque jamais des traitements puisque ce n'est qu'exceptionnellement qu'ils ne reposent pas sur une loi. L'exception de 16 al. 1 let. b doit être limitée aux cas où la loi prévoit une exception à l'information.<br><br>Si la proposition actuelle est retenue, il faudra expliquer ce que cela implique sur le principe de transparence. |

| Commentaire | Remarques (consultation) |
|---|---|
| Comme sur le plan fédéral (cf. art. 20 al. 2 LPD), l'alinéa 2 prévoit certaines autres exceptions, lorsque les données personnelles ne sont pas collectées auprès de la personne concernée. En pareil cas, le responsable du traitement peut notamment faire valoir l'impossibilité de donner l'information (par exemple parce que la personne concernée ne peut pas être identifiée malgré des recherches appropriées). La let. b prévoit également une exception spécifique lorsque l'information nécessite des efforts disproportionnés. Comme l'explique le Conseil fédéral dans son message explicatif relatif à la LPD, les efforts déployés pour informer la personne concernée sont disproportionnés dès lors qu'ils paraissent injustifiés par rapport au bénéfice que la personne concernée retirerait de l'information. L'information nécessite par exemple des efforts disproportionnés lorsque des données sont traitées uniquement à des fins d'archivage. Comme pour l'exception précédente, le responsable du traitement doit être actif dans la recherche de solutions pour communiquer l'information et fournir les efforts raisonnables dans le cas d'espèce. Ces deux dernières exceptions doivent être interprétées de manière restrictive dès lors qu'elles ne seront applicables que lorsque le traitement ne repose pas sur une base légale, ce qui devrait être l'exception. Cela revient à dire que l'application de l'alinéa 2 let. b tient à la quantité de travail qu'il sera nécessaire de fournir pour garantir la transmission de l'information versus l'intérêt des personnes concernées d'être informées et que les moyens mis en œuvre correspondent à ce qui peut légitimement être attendu, ce d'autant s'il s'agit de données sensibles.<br><br>L'alinéa 3 permet au responsable du traitement de renoncer, restreindre ou différer la communication des informations dès lors qu'une des conditions énumérées est réalisée. Les lettres a, c et d sont reprises de la loi actuelle. Ainsi la lettre a protège les intérêts de tiers qui pourraient subir un préjudice en cas de transmission de l'information. La lettre b traite des cas où la communication nuirait au traitement. On pense notamment à une procédure de contrôle en cours où informer du traitement reviendrait à prétériter la mise en œuvre des missions légales. La lettre c protège des intérêts publics lorsque les circonstances l'exigent. On retrouve cette notion également dans la loi vaudoise sur le droit à l'information à laquelle on peut se référer cas échéant. A relever cependant que cette exception doit être appréciée de façon objective, au terme d'une pesée des intérêts en jeu permettant de justifier le choix opéré. La lettre d reprend quant à elle l'exception liée à la communication d'informations susceptibles de compromettre une enquête, une instruction ou encore une procédure judiciaire ou administrative. Il s'agit ici de protéger des intérêts publics prépondérants dans un cadre bien déterminé. | |
| **Art. 17 Devoir d'informer en cas de décision individuelle automatisée**<br><br>La Confédération, à l'art. 21 LPD, a consacré une disposition à la problématique des décisions individuelles prises de façon entièrement automatisées. Cet article impose des obligations minimales aux responsables de traitements soumis à la LPD qui font usage de tels systèmes de décision, afin de respecter les exigences de l'art. 9 let. a de la Convention 108+ et de l'art. 11 de la directive (UE) 2016/680 (cf. art. 21 al. 2 LPD). | *Avis général : favorable avec complément et remarque*<br><br>L'expérience déjà vécue avec la LPD au niveau fédéral permet de constater que la limitation des règles en matière d'information aux seules « décisions » (soit ici des « décisions administratives ») peut laisser |

| Commentaire | Remarques (consultation) |
|---|---|
| Concrètement, l'art. 21 LPD concerne avant tout les personnes privées, qui établissent des relations de droit privé avec leurs clients (par exemple une entreprise d'assurance qui décide de proposer ou non la conclusion d'un contrat selon les informations personnelles fournies qu'un client lui a fournies). Les organes fédéraux agissant dans le cadre de procédures administratives régies par le droit public sont largement exemptés de ces obligations (cf. art. 21 al. 4 LPD), car les lois applicables à ces procédures prévoient déjà des exigences au moins aussi strictes. Ainsi, si une autorité rend une décision administrative (au sens de l'article 5 de la loi fédérale du 20 décembre 1968 sur la procédure administrative [PA ; RS 172.021] ou, sur le plan cantonal, de l'article 3 de la loi du 28 octobre 2008 sur la procédure administrative [LPA-VD ; BLV 173.36]) au terme d'un processus entièrement automatisé, cette décision pourra forcément être revue par une personne physique (comme l'exige l'art. 21 al. 2 LPD), sachant qu'elle pourra faire l'objet d'un recours devant un tribunal (art. 44 PA ; art. 92 LPA-VD), voire d'autres contestations préalables, comme une réclamation. De même, le droit d'être entendu préalablement à la décision (qui correspond à l'exigence de pouvoir « faire valoir son point de vue » de l'art. 21 al. 2 LPD) est aussi garanti par les lois de procédure, sous réserve de certaines exceptions particulières (cf. art. 30 PA ; art. 33 LPA-VD).<br><br>Dans ces conditions, comme la LPrD ne s'appliquera pas à des relations juridiques fondées sur le droit privé, une reprise à l'identique de l'art. 21 LPD n'apparait ni nécessaire, ni opportune. En matière de décisions individuelles automatisées, le présent projet se limite donc à prévoir l'obligation de signaler, par une mention expresse, les décisions administratives qui sont rendues au terme d'un processus entièrement automatisé (art. 17 al. 1 LPrD). En effet, cette obligation prévue par le droit supérieur est véritablement nouvelle et ne peut déjà être déduite de la LPA-VD, ni d'autres lois régissant les procédures administratives dans le canton de Vaud. L'autorité administrative qui recourt à un système automatisé pour rendre des décisions devra donc veiller à ce que lesdites décisions fassent mention du caractère automatique du traitement de données réalisé. Pour éviter toute lacune, l'art. 17 al. 2 et 3 LPrD rappelle néanmoins l'obligation de respecter le droit d'être entendu, sauf si la législation de procédure administrative l'exclut, ainsi que la nécessité de pouvoir soumettre les décisions au contrôle d'une personne physique, dans le cadre d'une réclamation ou d'un recours. | des lacunes, notamment lorsqu'un système automatisé est utilisé pour effectuer l'essentiel de l'analyse et rendre une évaluation, laquelle est ensuite utilisée pour qu'une personne physique rende effectivement une décision. Dans un tel cas, l'on ne parle pas de « décision automatisée », quand bien même l'influence de l'analyse effectuée automatiquement y est prédominante. En conséquence, il conviendrait d'étendre l'application de cette disposition aux décisions administratives et processus essentiellement automatisés, y compris lorsque la décision finale serait prise par une personne physique.<br><br>Par ailleurs, il conviendrait de préciser si la référence aux « décisions administratives » qui est utilisée ici correspond à la notion prévue dans la LPA-VD.<br><br>A l'instar de ce que prévoit le droit fribourgeois, il serait utile d'ajouter des dispositions dans la LPA-VD :<br>Art. XX Soutien automatisé à la prise de décision<br>1 Si une autorité utilise des algorithmes pour l'aider à former son raisonnement en fait ou en droit lors de la prise d'une décision, elle est tenue d'en faire mention systématiquement dans la partie de la décision qui contient la motivation.<br>2 A la demande du ou de la destinataire de la décision, l'autorité lui communique sous une forme intelligible la logique et les critères des algorithmes utilisés, à moins qu'un intérêt public prépondérant ne s'y oppose.<br>3 La demande n'a pas d'effet suspensif, sauf décision contraire de l'autorité, et elle n'entraîne aucune interruption de délai. |

| Commentaire | Remarques (consultation) |
|---|---|
| | Art. XX Décisions individuelles automatisées<br>1 Si une décision au sens de l'article 3 est prise sur le seul fondement d'un traitement de données personnelles automatisé, elle doit obligatoirement être présentée comme telle.<br>2 A la demande de la personne faisant l'objet d'une décision automatisée, l'organe qui a émis la décision lui communique sous une forme intelligible la logique et les critères à la base de celle-ci, à moins qu'un intérêt public prépondérant ne s'y oppose.<br>3 Sauf dans les cas où il n'existe pas de droit d'être entendu avant la décision, toute personne faisant l'objet d'une décision individuelle automatisée peut, dans les 30 jours, déposer une réclamation auprès de l'organe qui l'a émise, lorsque:<br>a) la décision est selon toute vraisemblance entachée d'une erreur non juridique, et<br>b) l'erreur en question est imputable à la machine qui l'a rendue.<br>4 L'organe qui a émis la décision procède à un réexamen sommaire et gratuit des opérations de traitement accomplies.<br><br>Pour les décisions individuelles automatisées qui ne sont pas des décisions au sens de l'art. 3 LPA- VD, une disposition similaire à celle de la LPD suffirait. |
| **Art. 18 Analyse d'impact**<br><br>L'analyse d'impact est une nouvelle obligation qui découle des exigences posées à l'art. 10 par. 2 de la Convention 108+ et des art. 27 ss de la directive (UE) 2016/680. L'art. 18 tel que proposé reprend en grande partie les dispositions de l'art. 22 LPD et pose les lignes directrices de la procédure. | *Avis général : favorable avec plusieurs observations*<br><br>Il convient d'ajouter à la liste des risques élevés (al. 2) le profilage, à l'image de ce qui se trouve dans l'essentiel des autres droits cantonaux. |

| Commentaire | Remarques (consultation) |
|---|---|
| Comme le relève le message explicatif relatif à la LPD, l'analyse d'impact est un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques. L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes juridiques liés à la protection des données et d'éviter les coûts qui pourraient en résulter.<br><br>Les alinéas 1 et 2 posent les règles et les motifs justifiant la réalisation d'une analyse d'impact. Il s'agit avant tout pour le responsable du traitement de faire une évaluation des conséquences que le traitement de données personnelles prévu peut avoir pour la personne concernée (droit à l'autodétermination, impact sur la personnalité, sur les droits fondamentaux, risque d'atteintes graves à la dignité par ex.).<br><br>Le risque sera considéré comme élevé en fonction de la nature, de l'étendue, des circonstances ou encore de la finalité du traitement. L'al. 2 donne deux exemples, bien sûr non exhaustifs (qui sont les mêmes que ceux prévus par l'art. 22 al. LPD) : let. a traitement d'un grand volume de données sensibles, comme cela peut être le cas dans le cadre de recherches sur la sécurité ; let. b surveillance systématique de grandes parties du domaine public, qui représente en soi un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées.<br><br>L'alinéa 3 fixe exigences minimales quant au contenu de l'analyse d'impact. Il reprend la liste du droit fédéral.<br><br>Les alinéas 4, 5 et 6 établissent la procédure cantonale en matière d'analyse d'impact, en s'inspirant largement de l'art. 23 LPD. Cette procédure permet à l'Autorité de de conseiller et de prévenir le responsable du traitement tout en garantissant le respect des principes de protection des données dès la conception. Les délais proposés sont identiques aux délais fédéraux et garantissent le bon déroulement de la procédure. L'Autorité évalue le traitement analysé et propose, cas échéant, des mesures permettant de respecter les dispositions de protection des données. Ces règles de procédure ne restreignent pas les pouvoirs de surveillance du chapitre VI l'Autorité restant libre d'ouvrir une enquête si le risque n'a pas été évalué correctement ou si les mesures ne suffisent pas à rendre le traitement conforme. | Il conviendra aussi de prévoir dans le Règlement que l'Autorité publie des listes noires (AIPD requise) et blanches (AIPD dispensée), ainsi qu'un modèle d'AIPD afin de simplifier l'appréciation des entités soumises à la LPrD. |
| **Art. 19 Communication de données personnelles**<br><br>L'art. 19 traite d'une forme particulière de traitement de données : la communication, opération qui, en soi, comporte des risques particuliers de porter atteinte à la personne concernée, notamment lorsqu'elle s'écarte de la finalité du traitement initial. | *Avis général : favorable avec une remarque*<br><br>La loi ou au moins le commentaire devrait préciser si la communication à un destinataire qui en a besoin pour l'accomplissement d'une tâche légale implique |

| Commentaire | Remarques (consultation) |
|---|---|
| Cet article reprend dans une large mesure les conditions de l'actuel art. 15 LPrD sur la communication. Le système prévu correspond par ailleurs à celui défini par l'art. 36 LPD sur le plan fédéral.<br><br>La règle est qu'une communication de données nécessite une base légale qui, si les données en cause sont sensibles, doit être de rang formel (art. 19 al. 1 let. a pLPrD). Lorsque la communication d'une donnée sensible est indispensable à l'accomplissement d'une tâche clairement définie dans une loi au sens formel (soit dans l'éventualité régie par l'art. 6 al. 2 let. b pLPrD pour les traitements de données en général), elle peut aussi se fonder sur base légale matérielle, si elle ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée (art. 19 al. 1 let. b pLPrD). L'art. 36 al. 1 LPD prévoit la même possibilité sur le plan fédéral, en renvoyant à l'art. 34 al. 3 LPD.<br><br>Au surplus, l'art. 19 al.1 let. a pLPrD permet la communication de données dans le cadre de la réalisation d'essais pilotes, au sens de l'art. 23 pLPrD. Si les conditions prévues par cette disposition sont remplies (cf. commentaire de l'art. 23 pLPrD ci-dessous), le Conseil d'Etat pourra ainsi autoriser la communication de données personnelles sensibles par l'intermédiaire d'une base légale matérielle (soit un arrêté, cf art. 23 pLPrD), pour la durée de l'essai pilote. Ceci pourra permettre, par exemple, d'expérimenter des procédures de simplification administrative mettant en œuvre le principe dit du « once-only » (qui vise à ne demander qu'une seule fois certaines indications aux individus et aux entreprises pour leurs démarches administratives, l'Etat s'occupant ensuite de transmettre ces informations aux différents services concernés) dans des domaines où certaines données sensibles sont traitées.<br><br>Les exceptions prévues par l'art. 19 al. 2 LPrD correspondent à la loi actuelle (let. b, d et e) ou à une situation de détresse que l'art. 36 LPD prévoit sur le plan fédéral (let. c, qui représente le pendant de l'art. 6 al. 3 let. a LPrD lorsque le traitement en cause est une communication de données).<br><br>L'alinéa 2 actuel n'est pas repris dans la présente proposition car les modifications proposées dans le cadre des travaux de mise à jour de la LInfo, plus particulièrement celles de l'art. 30 pLInfo, rendent obsolète ce renvoi.<br><br>Enfin, l'al. 3 est repris du droit actuel (art. 15 al. 3) dans une rédaction plus explicite. | une demande du destinataire (la loi révisée ne parle plus de requérant). |
| **Art. 20 Communication de données personnelles à l'étranger**<br><br>Cette disposition reprend, dans une large mesure, l'actuel art. 16 LPrD *Communication transfrontalière de données* et répond aux exigences de l'art. 14 de la Convention 108+ qui prévoit que des données personnelles ne puissent | *Avis général : favorable avec une nécessité de précisions*<br><br>L'alignement sur la LPD doit être salué. |

| Commentaire | Remarques (consultation) |
|---|---|
| être transmises à l'étranger que si l'état concerné offre un niveau approprié de protection des données. Le responsable du traitement devra se référer à la liste établie par le Conseil fédéral pour évaluer le niveau de protection des données offert par l'état concerné.<br>Al. 1 sans changement.<br>Al. 2 let. a, la notion de consentement exprès est reprise des nouvelles terminologies ; sans changement pour le reste des lettres a à f.<br>Let. g, reprend le droit actuel en complétant la liste des exemples de garanties suffisantes. La deuxième phrase répond quant à elle à l'obligation de l'art. 39 par. 3 de la directive (UE) 2016/680 qui prévoit que l'autorité responsable du contrôle doit être informée de tout transfert de données personnelles à des destinataires établis dans des pays tiers, lorsque ce transfert s'appuie sur l'existence de telles « garanties suffisantes ».<br>L'al. 2 est encore complété par une let. h prévoyant qu'une communication vers un pays tiers de données personnelles, faisant l'objet d'un traitement ou destinées à l'être, peut avoir lieu si un traité international garantit un niveau de protection approprié. Cette modification reprend l'art. 16 al. 2 let. a LPD qui permet la communication à l'étranger dès lors qu'un niveau de protection approprié est garanti par un traité international.<br>L'al. 3 donne la possibilité à l'Autorité de requérir des informations de la part des responsables de traitements qui communiquent des données à l'étranger, afin de pouvoir s'assurer que ces communications respectent les exigences légales.<br>L'al. 4 propose de poser un cadre clair à la communication de données personnelles à l'étranger. Avec cet alinéa, il est prévu, comme dans la loi fédérale (cf. art. 18 LPD) d'exclure la publication à des fins d'information du public – accès ouvert à toutes et tous - de données personnelles consultables depuis l'étranger la champ d'application de l'art. 20 pLPrD. Est visée ici la communication de données personnelles par Internet ou un autre service d'information accessible depuis l'étranger et répondant à une volonté d'informer le public. | L'al. 1 doit être complété pour indiquer que « La liste des pays adéquats figure à l'Annexe 1 OPDo », ce qui correspond à la pratique actuelle mais doit figurer dans la loi pour assurer la sécurité du droit.<br><br>Il conviendrait de faire explicitement référence, à l'al. 2 let. f, aux clauses types préalablement approuvées par le PFPDT (cf. art. 16 LPD et 10 OPDo) ou à l'éventuelle nécessité de les transposer au niveau cantonal.<br><br>Par ailleurs, dans le cas où l'entité se repose sur les garanties suffisantes selon l'al. 2 let. f, il ne suffit pas que l'Autorité soit informée, mais bien qu'elle approuve les garanties préalablement au transfert à l'étranger, en tout cas si le PFPDT n'a pas lui-même approuvé les garanties en question. A défaut d'une telle règle, un risque important existe quant à l'appréciation du niveau suffisant des garanties en question. |
| **Art. 21 Traitement des données personnelles par un sous-traitant**<br><br>L'art. 21 pLPrD remplace l'actuel art. 18 LPrD « Traitement de données par un tiers ». La notion de « tiers » y est remplacée par celle de sous-traitant, afin d'adapter la terminologie à celle du droit supérieur (cf. art. 9 LPD notamment), et clarifier les rôles. Pour mémoire, le sous-traitant est défini à l'art. 5 let. i pLPrD.<br>Al. 1 : sans changement, sous réserve du remplacement de la notion de tiers par celle sous-traitant.<br>Le nouvel al. 2 propose, sur la base du modèle fédéral (cf. art. 9 al. 2 et 41 LPD notamment), de rappeler clairement la responsabilité du responsable du traitement vis-à-vis de la personne concernée par un traitement de données, même si ce traitement est confié à un sous-traitant. Le responsable du traitement ne saurait en effet éluder sa responsabilité par le biais de la sous-traitance. Cette solution, d'une part, protège les intérêts de la personne concernée, qui pourra en tout temps s'adresser au responsable du traitement pour faire valoir ses droits procéduraux, | *Avis général : favorable avec observations*<br><br>A l'al. 1 « serait en droit » doit être remplacé par « est en droit » car le recours à un sous-traitant ne doit pas retirer le droit du responsable du traitement à continuer à traiter les données.<br><br>Pour éviter tout malentendu, le commentaire pourrait préciser que le secret de fonction ne s'oppose pas à la sous-traitance, même à l'étranger, si le sous-traitant est qualifié d'auxiliaire au sens du CP. |

| Commentaire | Remarques (consultation) |
|---|---|
| d'autre part, engage le responsable du traitement à prendre les dispositions nécessaires pour s'assurer que le sous-traitant respecte les mêmes principes de protection des données que lui. Comme le fait le droit fédéral, l'art. 21 met l'accent (« en particulier ») sur les règles de sécurité, mais le respect des autres devoirs prévus par la loi est bien sûr aussi exigé.<br>L'al. 3 du projet repend largement l'art. 9 al. 3 LPD, en ajoutant toutefois que l'autorisation préalable de « sous-sous-traitance » doit être donnée sous forme écrite. Cette exigence de la forme écrite s'impose pour des raisons de sécurité, mais également de conformité à l'art. 22 par. 2 directive (UE) 2016/680.<br>L'alinéa 4 prévoit l'obligation pour le sous-traitant de collaborer et d'aider le responsable du traitement, lorsqu'une personne concernée fait valoir des droits procéduraux (art. 26 à 31 pLPrD) au sujet de données personnelles qu'il traite pour le compte de ce dernier. Cette obligation vient compléter, si nécessaire, les règles contractuelles qui lient le sous-traitant au responsable du traitement, dans l'intérêt des personnes concernées, qui ne doivent pas voir leurs droits restreints par des obstacles relevant de la relation juridique entre responsable du traitement et sous-traitant. La deuxième partie de la phrase permet au responsable du traitement d'autoriser le sous-traitant à répondre directement é une demande d'accès (art. 26 pLPrD). Ceci ne change rien au fait que le responsable du traitement est, vis-à-vis de la personne concernée, le débiteur de ce droit d'accès (art. 26 al. 4 pLPrD). | Le contenu minimal du contrat devrait être prévu soit dans la loi, soit *a minima* dans le Règlement. Une précision en ce sens devrait être ajoutée.<br>On ajoutera également que le contrat doit être écrit, y compris en la forme électronique. Cela n'oblige pas à avoir une signature, mais évite les accords oraux. |
| **Art. 22 Obligation d'annoncer les violations de la sécurité des données**<br><br>La disposition consacrée à l'obligation d'annoncer les violations de la sécurité des données est reprise largement de l'art. 24 LPD. Comme sur le plan fédéral, cette obligation d'annonce vise à répondre aux exigences du droit supérieur telles qu'elles ressortent notamment des art. 7 par. 2 de la Convention 108+, des art. 30 s de la directive (UE) 2016/680. L'article permet ainsi de mettre le droit cantonal en conformité à ce qui est attendu.<br>L'al. 1 prévoit que le responsable du traitement annonce dans les meilleurs délais à l'Autorité toute violation de la sécurité des données personnelles, s'il est vraisemblable qu'elle entraîne un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Ceci correspond au texte de l'art. 24 al. 1 LPD. La notion de violation de la sécurité est définie dans le présent projet à l'art. 5 al. 1 let. j comme une atteinte au principe de sécurité, sans égard au fait qu'elle soit accidentelle ou illicite, entrainant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non-autorisé à ces données. La réalité montre que la perte de maitrise entraînée par la violation de la sécurité peut faire encourir un risque d'utilisation abusive des données personnelles ainsi obtenues. On pense ici notamment à des attaques de tiers, comme ce fût le cas en mai 2021, lors d'une cyberattaque contre une commune qui a fait l'objet d'une importante médiatisation, mais l'atteinte peut aussi être due à des actions de personnes internes à l'entité concernée qui, par négligence ou volontairement, contreviennent aux règles de sécurité et de protection des données. | *Avis général : favorable avec plusieurs observations*<br><br>A l'alinéa 1, la formulation est jugée malheureuse et laissant une trop grande marge d'interprétation : « dans les meilleurs délais ». En effet, soit il y a une obligation d'annonce devant être immédiate en cas de violation, soit il y a un délai précis pour ce faire. Il faut laisser le temps aux responsables d'évaluer le risque d'atteinte aux droits fondamentaux. Ayant besoin d'un moment de réflexion, c'est pour cette raison qu'il n'a pas été mentionné « immédiatement ». Il faudrait mentionner : « dès que possible » ou « sans tarder », soit une formulation plus ouverte sans l'être plus que : « dans les meilleurs délais ».<br><br>Il n'y a pas mention de la restriction de l'information s'il existe un devoir légal de garder un secret, quand bien même le message indique que ceci découle de la réserve de la loi au sens formel de l'al. 5 let. a (cf. art. |

| Commentaire | Remarques (consultation) |
|---|---|
| Dès que le traitement non autorisé est connu (dans les meilleurs délais), le responsable du traitement doit évaluer s'il existe un risque élevé d'atteinte aux droits fondamentaux des personnes concernées. C'est seulement lorsque que cette atteinte n'est pas vraisemblable que le responsable du traitement puisse s'abstenir d'en informer l'Autorité.<br>L'al. 2 précise le contenu minimum de l'annonce à l'Autorité. Doivent y figurer : la nature de la violation à savoir la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non-autorisé à ces données (cf. définition de l'art. 5 al. 1 let. j) ; ses conséquences, l'annonce doit mettre en avant les conséquences de la violation non seulement pour le responsable du traitement mais surtout pour la personne concernée et les mesures prises ou prévues, à savoir ce qui va, ou peut, être entrepris pour soit remédier à la violation soit atténuer les conséquences.<br>L'al. 3 concerne le sous-traitant qui rencontre un cas de violation de la sécurité des données personnelles. Le sous-traitant a l'obligation d'informer le responsable du traitement de tous les cas de violation de la sécurité des données au sens de l'art. 5 al. 1 let. j, peu importe le degré de risque qu'ils entraînent. C'est ensuite au responsable du traitement d'évaluer si le risque est suffisamment élevé et vraisemblable pour qu'une annonce soit faite, au sens de l'alinéa 1. Le sous-traitant devra ainsi tout mettre en œuvre pour que le responsable du traitement puisse répondre à ses obligations légales.<br>L'al. 4 traite de l'information faite à la personne concernée lorsque le responsable du traitement estime que cette mesure est nécessaire pour lui permettre de prendre des mesures pour protéger ses droits fondamentaux (changement de profil, clôture d'un compte, modification du mot de passe, annonce à la banque, par ex.) ou que l'Autorité le demande.<br>L'al. 5 traite des exceptions au devoir d'annonce. La première éventualité correspond au cas dans lequel une base légale formelle l'interdit, par exemple en prévoyant une obligation de respecter le secret. Le deuxième cas de figure est celui dans lequel un intérêt public ou privé prépondérant l'exige (lorsqu'une procédure est en cours, par ex.). Une pesée des intérêts soigneuse sera donc nécessaire. La troisième exception relève de l'impossibilité d'informer. Ce sera notamment le cas lorsque les données ont été effacées et qu'il est impossible d'identifier la personne concernée, ou lorsqu'il faudrait engager, par rapport aux risques encourus, des moyens disproportionnés pour atteindre les personnes concernées. Enfin, la let. d autorise le responsable du traitement à informer les personne concernée par une communication publique, si ce type de communication se révèle plus opportun qu'une information personnelle. | 24 al. 5 let. a LPD). Ceci n'est toutefois pas entièrement correct, dans la mesure où le secret ne constitue pas un cas d'exclusion prévu expressément par une loi au sens formel, mais une restriction générale. Une mention explicite y relative devrait donc être ajoutée.<br><br>Une exclusion de l'utilisation des informations transmises dans le cadre d'une procédure pénale, en ligne avec ce que prévoit l'art. 24 al. 6 LPD, devrait aussi être ajoutée.<br><br>Il serait également nécessaire de prévoir une obligation pour l'entité concernée de documenter la violation de la sécurité des données ainsi que les mesures mises en place pour y remédier, lorsqu'il s'agit d'une violation devant être annoncée.<br><br>Contrairement à ce qu'indique le commentaire, l'al. 5 concerne seulement le cas de l'information aux personnes concernées (al. 4) et pas l'annonce à l'Autorité (al. 3).<br><br>La fin de l'al. 4 « lorsque l'Autorité le demande » peut être supprimé car il donne faussement l'impression que l'Autorité peut le demander si cela n'est pas nécessaire à la protection des personnes concernées (et sans que la loi n'indique quand). |
| **Art. 23 Traitement de données personnelles dans le cadre d'essais pilotes**<br>Cette disposition nouvelle vise à permettre à l'Etat, sur la base d'un arrêté du Conseil d'Etat, de réaliser des essais pilotes dans des domaines qui nécessitent le traitement de données personnelles sensibles. Une disposition similaire existe dans le droit fédéral (art. 35 LPD). Ce dispositif permettra au Conseil d'Etat d'évaluer soigneusement l'intérêt | *Avis général : favorable avec deux compléments*<br><br>La simple consultation de l'Autorité (al. 3) doit être remplacée par un préavis favorable. |

| Commentaire | Remarques (consultation) |
|---|---|
| ainsi que les risques d'un nouveau traitement de données sensibles dans un domaine d'activité étatique donné, avant de proposer éventuellement au Grand Conseil d'adopter une loi formelle pérennisant ce traitement. On pourrait concevoir, par exemple, qu'un essai pilote soit mené concernant un dispositif d'accès à certaines prestations étatiques par l'intermédiaire d'un système d'identification biométrique.<br>L'al. 2 encadre la réalisation d'un tel essai de manière très stricte. Premièrement, la tâche dont le traitement envisagé relève doit figurer dans une base légale formelle (la nuance par rapport à l'art. 6 al. 2 let. b pLPrD étant que le traitement n'est pas « absolument indispensable » à l'accomplissement de cette tâche). Il est donc exclu que le Conseil d'Etat prévoie un essai pilote dans un domaine qui n'est pas déjà régi par le Canton, en vertu d'une loi au sens formel. Deuxièmement, il appartient au Conseil d'Etat de veiller à ce que des mesures visant à réduire au minimum les atteintes aux droits fondamentaux soient prises (notamment des mesures techniques pour garantir la sécurité des données ou organisationnelles pour réduire les risques de violation ou encore procédurales pour codifier l'accès aux données personnelles par ex.). De façon générale, le Conseil d'Etat veillera attentivement au respect des principes généraux de protection des données personnelles (proportionnalité, finalité, exactitude, sécurité, …). Troisièmement, la phase pilote doit être indispensable, en particulier pour des raisons techniques. Le traitement particulier est nécessaire pour résoudre des situations où les solutions techniques ne sont pas encore clairement identifiées ou nécessiteraient d'être testées. Il peut en être de même pour les solutions organisationnelles à mettre en œuvre. En d'autres termes, la phase d'essai pilote ne doit pas être justifiée par des motifs de pure convenance : Il faut que des motifs légitimes la justifient.<br>L'al. 3 exige que l'Autorité soit consultée préalablement à tout essai pilote, sa détermination étant transmise au Conseil d'Etat. En effet, il importe que le Gouvernement cantonal soit dûment renseigné sur la prise de position de l'Autorité (en sa qualité d'expert) avant de prendre la décision d'autoriser, ou non, un essai pilote.<br>L'al. 4 prévoit une obligation pour le responsable du traitement de transmettre dans un délai de deux ans au maximum après la mise en œuvre de la phase d'essai, un rapport d'évaluation concluant à la poursuite ou à l'interruption du traitement. L'Autorité doit être invitée à prendre position dans ce cadre. Cette obligation de bilan intermédiaire permet de cadrer le traitement testé. Ainsi, selon la conclusion du responsable du traitement, le rapport pourra servir à l'élaboration du projet de loi formelle ou, au contraire, sonner la fin de la phase pilote ou encore mettre en évidence des besoins complémentaires en vue de la finalisation de la phase d'essai.<br>L'al. 5 prévoit que si aucune loi au sens de l'art. 6 al. 2 n'est entrée en vigueur au terme du délai de cinq ans à compter de la mise en œuvre de l'essai pilote, ce traitement particulier doit être interrompu. Cette disposition garantit que l'essai ne perdure pas dans le temps : Si le traitement donne satisfaction, il reviendra au Conseil d'Etat de proposer au Grand Conseil l'adoption des bases légales nécessaires à le pérenniser. Ce délai correspond à celui prévu par l'art. 35 al. 4 LPD. | Le rapport au sens de l'al. 4 doit être rendu public. Il convient de le préciser explicitement.<br><br>Le délai de 5 ans prévu à l'al. 5 paraît trop long pour un canton (c'est le délai mis en œuvre au niveau fédéral – mais doit être plus court au niveau cantonal). Il conviendrait de prévoir un délai maximal de 3 ans pour l'adaptation des bases légales. |
| **Art. 24 Conservation des données personnelles et proposition aux Archives cantonales** | *Avis général : favorable* |

| Commentaire | Remarques (consultation) |
|---|---|
| Cette disposition reprend les règles de l'actuel art. 11 *Conservation*.<br>Al. 1 Sans changement.<br>Al. 2 Référence directe est faite à la loi cantonale sur l'archivage ; pour le surplus sans changement. | |
| **Art. 25 Statistiques, planification et recherche**<br><br>Cette disposition reprend partiellement l'art. 24 actuel et pour le surplus, se calque sur les dispositions similaires du droit fédéral et des législations cantonales en cadrant la communication uniquement à des fins ne se rapportant pas à des personnes.<br>Al. 1 let. b introduit une nouvelle obligation pour le responsable du traitement qui ne peut communiquer des données sensibles que sous une forme ne permettant pas d'identifier la personnes concernée. Conformément au droit fédéral, cette modification vient renforcer la protection des données sensibles. Pour le surplus, les let. a, c et d sont sans changement.<br>Les références de l'al. 2 sont mises à jour. | *Avis général : favorable avec une observation*<br><br>Remplacer « **but** de leur traitement » par « **finalité** du traitement » pour plus de cohérence avec le reste de la terminologie de la loi. Le commentaire devrait aussi préciser qu'il s'agit d'une utilisation secondaire des données et que cette disposition permet de traiter des données déjà collectées par l'entité (dans le respect de l'art. 6 notamment) mais pas de collecter de nouvelles données dans un but statistique. |
| **Chapitre IV Droits de la personne concernée** | |
| **Art. 26 Droit d'accès à ses propres données**<br><br>Cette disposition reprend la notion du droit d'accès déjà connue dans le droit en vigueur et l'adapte à l'évolution du droit supérieur (art. 9 par. 1 let. b et c Convention 108+ et de l'art. 14 directive (UE) 2016/680). De façon générale, cet article se veut similaire à l'art. 25 LPD et son interprétation pourra s'appuyer sur celle que le Tribunal fédéral fait de cette dernière disposition.<br><br>Le droit d'accès est et reste l'institution centrale du droit de la protection des données. Il est la clé de voûte qui permet à la personne concernée de faire valoir les droits que lui octroie la loi. Il est d'ailleurs ancré à l'art. 15 al. 2 let. a Cst-VD. Sans droit d'accès, la personne concernée ne serait en effet pas en mesure d'exercer ses droits en matière de protection des données. Seul·e celui ou celle qui a connaissance d'un traitement de données le ou la concernant est à même, le cas échéant, d'en vérifier le but, voire d'en demander la rectification ou la suppression si des données inexactes ou sans lien avec le but du traitement sont traitées. Le droit d'accès complète l'obligation d'informer du responsable du traitement prévue à l'art. 15 pLPrD. Les personnes concernées peuvent identifier le | *Avis général : favorable avec deux modifications*<br><br>La notion de « libre accès » est trop large et doit être remplacée par « Toute personne peut demander au responsable du traitement si des données personnelles la concernant sont traitées. ».<br><br>L'al. 2 let. f doit être complété avec « la logique sur laquelle se base la décision ». |

| Commentaire | Remarques (consultation) |
|---|---|
| responsable du traitement des données qu'elles cherchent grâce au registre des activités de traitement (art. 48 pLPrD).<br>Selon l'al. 1, toute personne a, en tout temps, libre accès aux données la concernant. Le droit d'accès appartient à toute personne physique qui fait l'objet d'un traitement et ne dépend donc d'aucun intérêt particulier. Cela signifie qu'il n'y a aucune restriction liée à la nationalité, au domicile ou à l'âge, voire à la personnalité du demandeur ou à ses motivations et à l'usage qu'il compte faire de ses données. Le demandeur n'a, en outre, pas à motiver sa demande.<br>L'al. 2 met en lumière tant le lien étroit qui existe entre le droit d'accès et le devoir d'informer que le but fondamental du droit d'accès qui est de permettre à la personne concernée de faire valoir ses droits, ATF 138 III 425, consid. 5.3. Il précise également le contenu du droit d'accès. Les let. a à g énumèrent les informations qui doivent au minimum être communiquées à la personne concernée. La norme générale contenue dans la phrase introductive permet subsidiairement à la personne concernée de demander d'autres informations qui sont nécessaires pour qu'elle puisse faire valoir ses droits en vertu de la LPrD et pour garantir la transparence du traitement.<br>La personne concernée doit dans tous les cas recevoir des informations sur l'identité et les coordonnées du responsable du traitement (let. a). Selon les cas, il est possible qu'elle dispose déjà d'une telle information (dans le cadre du devoir d'information, par ex.). Elle en recevra donc seulement confirmation. Il est toutefois aussi possible que la personne concernée ne connaisse l'identité du responsable du traitement qu'à ce moment-là (par ex. en cas de pluralité de responsables du traitement). Par ailleurs, la personne concernée doit être informée des données personnelles traitées en tant que telles (let. b) ainsi que de la finalité et la base légale du traitement (let. c). Elle doit également être informée de la durée de conservation des données ou, si cela n'est pas possible, des critères pour fixer cette dernière (let. d). Cette information lui permet notamment de savoir si le responsable du traitement conserve les données conformément aux principes prévus aux art. 6 ss pLPrD. Comme la durée de conservation des données n'est pas toujours communiquée dans le cadre du devoir d'informer, la personne concernée doit, dans tous les cas, recevoir cette information lorsqu'elle exerce son droit d'accès. Elle reçoit également les renseignements disponibles sur l'origine des données, dans la mesure bien sûr où elle n'a pas fourni elle-même ces données (let. e), et est informée, le cas échéant, de l'existence d'une décision individuelle automatisée (let. f). Enfin, il y a lieu d'indiquer également à la personne concernée les destinataires ou les catégories de destinataires auxquels les données ont éventuellement été communiquées (let. g). Si les destinataires se trouvent à l'étranger, l'information | |

| Commentaire | Remarques (consultation) |
|---|---|
| doit spécifier l'Etat concerné et, le cas échéant, les garanties prévues au sens de l'art. 15, al. 3 pLPrD, ou l'application d'une des exceptions de l'art. 16 pLPrD.<br>Le droit d'accès doit également permettre à la personne concernée, le cas échéant, d'avoir la confirmation que ces données n'existent pas (al. 3).<br>Le débiteur du droit d'accès est toujours le responsable du traitement au sens de l'art. 5 al. 1 let. h pLPrD. Le fait que celui-ci confie le traitement à un tiers ne change rien à cet égard (al. 4). Lorsque la personne concernée adresse une demande d'accès directement au sous-traitant, celui-ci doit lui indiquer le nom du responsable du traitement ou transmettre directement sa demande à ce dernier. S'il n'est pas tenu, en pareil cas, de renseigner lui-même la personne concernée, le sous-traitant ne doit pas non plus entraver l'exercice du droit d'accès, FF 2017 6565, p. 6684.<br>Comme dans le droit actuel, il incombe au demandeur de s'assurer de l'identité du requérant afin que seules ses propres données lui soient effectivement transmises, au besoin par la présentation de pièces justificatives (al. 5). En pratique, une copie du document d'identité est souvent demandée. Elle doit être détruite dès que la vérification a été réalisée. En outre, nul ne peut renoncer par avance au droit d'accès (al. 6).<br>S'agissant de l'accès aux données des personnes décédées, il ne parait pas essentiel de légiférer sur ce point. En effet, la CDAP a été amenée à trancher la question, cf. GE.2016.0084. | |
| **Art. 27 Modalités**<br><br>La teneur de cette disposition ne subit pas de modification drastique par rapport au droit actuel. La demande n'est soumise à aucune exigence de forme (al. 1). Lorsqu'il traite des quantités importantes de données sur la personne concernée, le responsable du traitement peut demander à cette dernière de préciser sur quelles données ou quelles opérations de traitement porte sa requête, comme cela est le cas en droit fédéral, FF 2017 6565, p. 6683. La personne concernée a désormais le droit d'obtenir une copie des données la concernant (al. 2), comme cela a été retenu par le Tribunal fédéral s'agissant de la LPD, ATF 141 III 119. La règle est que les données sont généralement communiquées par écrit. Avec l'accord du requérant toutefois, elles peuvent être transmises par oral ou par l'intermédiaire d'un moyen électronique. La notion de moyen électronique est plus large que celle de voie électronique au sens de l'art. 27a LPA-VD. Les renseignements doivent, dans tous les cas, être remis sous une forme compréhensible. | *Avis général : favorable avec deux observations et une modification*<br><br>L'al. 1pourrait être complété par « à la demande du responsable du traitement, il confirme sa demande par écrit ».<br><br>Le terme demandes répétitives doit être remplacé par demandes répétées.<br><br>A l'alinéa 4, il faudrait prévoir plutôt la formulation suivante : « Le droit d'accès est, en principe, gratuit ». Autrement, le danger est de déléguer au Conseil d'Etat la possibilité de créer une liste d'exceptions pouvant potentiellement relever d'un inventaire disparate dans un règlement. |

| Commentaire | Remarques (consultation) |
|---|---|
| Le droit d'accès est en principe gratuit. Il peut toutefois être perçu un émolument lorsque la communication requiert un travail considérable ou en cas de demandes répétitives. Le Conseil d'Etat conserve le droit de fixer le tarif des émoluments. | |
| **Art. 28 Délais**<br><br>A l'exception d'une adaptation rédactionnelle, la teneur de la disposition ne subit pas de modification par rapport au droit actuel (art. 26a LPrD). | *Avis général : favorable avec un complément*<br><br>Le délai de 30 jours devrait être prolongeable si la demande est trop importante ou que la réponse exige un travail considérable, à l'image de ce qui existe en droit fédéral. |
| **Art. 29 Restrictions**<br><br>Comme dans le droit actuel, le droit d'accès n'est pas illimité. L'art. 29 al. 1 du projet énonce les conditions auxquelles il peut être restreint, voire refusé. L'invocation d'un motif de restriction ou de refus au droit d'accès doit toutefois rester l'exception. Elle ne peut avoir lieu que de manière restrictive après avoir procédé à une pesée des intérêts en présence et conformément au principe de proportionnalité.<br><br>Le droit d'accès peut tout d'abord être restreint ou refusé lorsqu'une loi le prévoit expressément. L'accès peut également être restreint ou refusé au cas où un intérêt public ou privé prépondérant 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. Il arrive au demeurant que la protection de la personne elle-même justifie une restriction ou un refus au droit d'accès.<br><br>Finalement, seule nouveauté, le droit d'accès peut être refusé ou restreint lorsque la demande d'accès est manifestement infondée notamment parce qu'elle poursuit un but contraire à la protection des données ou est manifestement procédurière. S'agissant des demandes « manifestement infondées », la terminologie reprend celle utilisée, par exemple, à l'art. 108 LTF. Par cela, il faut entendre les cas typiques d'abus de droit, soit l'exercice d'un droit à des fins étrangères à son but. Le fardeau de la preuve des circonstances permettant de conclure à l'abus de droit incombe au responsable du traitement qui entend s'en prévaloir, cf. BENHAMOU Yaniv, dans le Commentaire Romand de la loi fédérale sur la protection des données, 2023, n° 15 ad art. 26 LPD. Le Tribunal fédéral a déjà eu l'opportunité de trancher à plusieurs reprises ce qui devait être ou non considéré comme une | *Avis général : favorable avec des modifications*<br><br>Il faudrait une loi au sens formel pour pouvoir restreindre l'accès (et non pas simplement une loi – cf. art. 26 LPD).<br><br>La loi doit être complétée pour indiquer que le motif doit être communiqué (cf. art. 26 al. 4 LPD).<br><br>Lorsque le motif disparait, le demandeur doit en être informé et il doit confirmer le maintien de sa demande d'accès. Cela évite à l'autorité de consacrer un temps important à une demande qui n'est peut-être plus pertinente. L'al. 2 doit être modifié dans ce sens. |

| Commentaire | Remarques (consultation) |
|---|---|
| demande abusive (Voir notamment ATF 141 III 119 et ATF 138 III 425). En ce qui concerne les demandes « manifestement procédurières », elles s'entendent comme les demandes introduites par pur esprit de chicane dans le but de tracasser l'adversaire et de le solliciter inutilement (par ex., des demandes d'accès successives qui seraient adressées au même responsable du traitement alors que le demandeur sait pertinemment qu'aucune donnée personnelle le concernant n'est traitée par le responsable du traitement en question) cf. également BENHAMOU Yaniv, dans le Commentaire Romand de la loi fédérale sur la protection des données, 2023, n° 18 ad art. 26. Cette exception ne pourra toutefois être soulevée que dans les cas particulièrement choquants et dûment avérés. Ainsi, comme le relève la doctrine, on ne saurait automatiquement considérer qu'une relation conflictuelle de droit du travail par exemple atteste systématiquement de la volonté du demandeur d'exercer son droit d'accès de manière chicanière, cf. DI TRIA Livio, LUBISHTANI Kastriot, Etude empirique du droit d'accès, in Le droit d'accès, 2021. Comme en droit fédéral (art. 26 al. 1 let. c LPD), le responsable du traitement ne doit donc pas conclure à la légère au caractère manifestement infondé, voire procédurier, de la demande. De plus, il lui appartient de choisir l'option la plus favorable pour la personne concernée en se contentant de restreindre la communication, voire de la différer, lorsque cela est possible.<br><br>De manière générale, les données personnelles de tiers doivent être caviardées. Une telle mesure n'est toutefois pas toujours suffisante pour les protéger.<br><br>Une remarque doit encore être faite au sujet de l'actuel art. 27 al. 2 LPrD, qui n'est pas repris dans le projet de loi.<br><br>Le droit d'accès d'un patient aux données de son dossier détenu par un professionnel de la santé est régi par l'art. 24 LSP, qui constitue une loi spéciale dérogeant au régime général prévu par les art. 25 ss LPrD. Selon cet art. 24 LSP, l'accès au dossier du patient est garanti (et s'accompagne du droit de recevoir des explications de la part du professionnel de la santé ; art. 24 al. 1 LSP) mais il peut, aux conditions de l'art. 24 al. 3 LSP, être soumis à certaines modalités particulières, dans l'intérêt du patient lui-même.<br><br>L'art. 27 al. 2 LPrD actuel réservait ce cas particulier. Après analyse, il n'apparaît pas nécessaire de reprendre une telle disposition dans la nouvelle loi, pour deux motifs au moins : 1) En vertu des principes généraux du droit, la loi spéciale (LSP) déroge à la loi générale (LPrD) sans qu'il soit nécessaire de le dire et 2), surtout, l'art. 27 al. 2 | |

| Commentaire | Remarques (consultation) |
|---|---|
| LPrD actuel se réfère à « *l'accès aux données médicales* » de façon trop générale, sachant que l'art. 24 LSP se borne à réglementer la problématique de l'accès par un patient à son propre dossier médical détenu par un professionnel de la santé (et non pas toutes les situations dans lesquelles l'accès à des « données médicales » pourrait être demandé, par exemple auprès d'un assurance ou d'une administration). Ceci génère une incertitude quant à la portée de cette réserve, que la présente révision permet de supprimer. | |
| **Art. 30 Droit d'opposition**<br><br>Comme dans le droit actuel, le droit d'opposition permet à la personne rendant vraisemblable un intérêt digne de protection de s'opposer par avance à la communication de certaines données la concernant. Le droit d'opposition fait partie des prétentions que le droit supérieur reconnaît de manière générale aux personnes concernées, sans égard au type de données visées (cf. art. 9 par. 1 let. d convention 108+).<br>Le texte de cet article correspondant à celui de l'art. 37 LPD, sa mise en œuvre suivra les mêmes principes. Cela signifie notamment que la personne concernée devra faire valoir un intérêt légitime à s'opposer à la transmission des données qui le concernent. Dans le cas contraire, son opposition sera levée. L'intérêt légitime fera en particulier défaut si l'opposition apparaît essentiellement motivée par la volonté d'échapper à des obligations juridiques, comme celle de payer une taxe ou de subir une sanction administrative (voir également l'art. 19 al. 2 let. e pLPrD, qui est basé sur les mêmes considérations). L'opposition sera par ailleurs toujours levée lorsque la communication de données est imposée par la loi (art. 30 al. 2 let. a pLPrD). En effet, dans une telle situation, c'est le législateur qui aura procédé préalablement à la pesée des intérêts en présence et fait prévaloir l'intérêt public à la communication. Enfin, le responsable du traitement pourra lever l'opposition lorsque celle-ci risque de compromettre l'accomplissement de ses tâches (art. 30 al. 2 let. b pLPrD). Il devra alors procéder à une pesée des intérêts, démontrant que celui à l'accomplissement des tâches en question prime celui que la personne concernée fait valoir à ce que ses données ne soient pas communiquées. | |
| **Art. 31 Autres droits**<br><br>A l'exception de la suppression de l'actuel art. 29 al. 1 let. d LPrD, la teneur de la disposition ne subit pas de modification par rapport au droit en vigueur.<br>L'al. 1er énonce les trois moyens défensifs traditionnels pouvant être invoqués en cas d'atteinte ou de risque d'atteinte aux droits des personnes imputable à un traitement illicite de données. L'al. 2 contient une liste non exhaustive des demandes plus précises que les personnes ayant un intérêt digne de protection peuvent formuler. Le | |

| Commentaire | Remarques (consultation) |
|---|---|
| choix entre la rectification, la destruction ou l'anonymisation des données revient au demandeur. Lorsque l'exactitude ou l'inexactitude d'une donnée ne peut être établie, le responsable du traitement ajoute à la donnée la mention de son caractère litigieux (al. 3).<br>Comme cela est déjà le cas dans le droit actuel, les droits prévus par cette disposition peuvent aussi bien être invoqués par la personne physique concernée, qui dispose systématiquement d'un intérêt digne de protection, que par toute autre personne ou entité ayant un intérêt digne de protection. Ainsi, les personnes habilitées à invoquer l'une ou l'autre prétention prévue dans l'art. 31 peuvent être les proches de la personne concernée (par exemple, les descendants de personnes décédées) ou encore certaines associations lorsqu'elles agissent pour défendre leurs intérêts idéaux ou ceux de leurs membres. On retrouve une solution identique dans la loi actuelle (art. 29 LPrD) qu'en droit fédéral (art. 41 LPD). Le choix entre la rectification, la destruction ou l'anonymisation des données revient à la personne concernée.<br>La suppression de la disposition selon laquelle les personnes qui ont un intérêt digne de protection peuvent exiger du responsable du traitement qu'il répare les conséquences d'un traitement illicite de données vise à supprimer la confusion que sa portée engendre à l'heure actuelle. A la lecture de l'actuel art. 29 al. 1 let. d LPrD, il n'est en effet pas clair si l'action en responsabilité contre l'Etat doit faire l'objet d'une procédure séparée (FR, par ex.) ou si elle est intégrée à la procédure de protection des données, l'autorité saisie devant dans un tel cas statuer simultanément sur l'éventuel caractère illicite d'une atteinte et les demandes de dommages-intérêts et de réparation du tort moral (ZG, par ex.). La CDAP a toutefois tranché la question et estimé que de telles prétentions relèvent de la loi du 16 mai 1961 sur la responsabilité de l'Etat, des communes et de leurs agents (LRECA ; BLV 170.11). Elles sont donc de la compétence des tribunaux « ordinaires », c'est-à-dire civils en application de l'art. 14 LRECA, cf. arrêt de la CDAP du 16 décembre 2016 GE.2016.0084 et arrêt de la CDAP du 30 juin 2022 GE.2022.0114. Il convenait dès lors de clarifier la situation. | |
| **Chapitre V Autorité et Préposé**<br><br>En complément de l'article 3 du présent projet qui pose le principe et la mission générale de l'Autorité de protection des données et de droit à l'information, les dispositions du chapitre V détaillent plus précisément les règles organisationnelles applicables. Comme relevé au commentaire de l'art. 3, le projet prévoit d'instaurer l'Autorité dans son ensemble comme chargée de la bonne exécution du droit cantonal en matière de protection des données en lieu et place de l'actuel notion de Préposé. Cette façon de procéder reprend la systématique de la loi fédérale en la matière. En effet, lorsque la LPD se réfère au chef du Préposé fédéral à la protection des données et à la | |

| Commentaire | Remarques (consultation) |
|---|---|
| transparence en tant que personne, elle parle du « préposé » et lorsque la loi se réfère au « préposé fédéral à la protection des données et à la transparence (PFPDT) il s'agit de l'autorité dans son ensemble. | |
| **Art. 32 Désignation et statut**<br><br>Le droit actuel est peu clair s'agissant du mandat du Préposé et nécessite d'être précisé, notamment en ce qui concerne sa mise en œuvre (cf. également commentaire des art. 33 s infra). Le projet propose d'organiser la fonction, notamment en respect de ce qui est attendu dans le cadre de l'évaluation Schengen où la Suisse s'est vue recommandée d'être plus précise quant à l'indépendance, au rôle et aux compétences des autorités en charge de la protection des données.<br>L'art. 32 reprend donc les dispositions de l'art. 34 LPrD et pour le surplus s'inspire du droit fédéral en la matière, cf. art. 43 ss LPD.<br>Al. 1, le projet prévoit que la durée de fonction du Préposé sera désormais de cinq ans. Cette modification vise à harmoniser la durée de la fonction du Préposé avec celle qui est déjà prévue pour les membres du Grand Conseil, du Tribunal cantonal et du Conseil d'Etat.<br>L'al. 2, quant à lui, prévoit un unique renouvellement du mandat (cinq ans). Cette solution permet de répondre non seulement aux exigences de l'art. 44 par. 1 let. e de la directive (UE) 2016/680 *les Etats Schengen doivent régler le caractère renouvelable ou non du mandat du Préposé et cas échéant le nombre de mandats* mais également à celles posées par l'art. 15 par. 5 de la Convention 108+ qui prévoit une degré d'indépendance des autorités de contrôle suffisant pour protéger efficacement les droits et libertés individuels. Cette indépendance se traduit notamment par la durée d'exercice du mandat. Le fait de pouvoir rester en fonction 10 ans permet de garantir une forme de sécurité et ainsi renforcer l'indépendance du Préposé. La durée de 10 ans paraît raisonnable compte tenu de l'expertise nécessaire et attendue (cf. commentaire de l'alinéa 3) et pose une limite à la proximité qui pourrait s'installer au fil du temps avec les entités sur lesquelles le contrôle s'effectue.<br>Avec l'alinéa 3 le projet vise à requérir un niveau de compétence professionnelle minimum pour pouvoir prétendre à la fonction de Préposé. Cette exigence constitue un gage de l'indépendance de l'Autorité. En effet, l'étendue des tâches et pouvoirs liés à la fonction rendent nécessaire que la personne élue au poste de Préposé cantonal à la protection des données et au droit à l'information bénéficie de compétences et connaissances adéquates. Une formation juridique paraît être un minimum.<br>L'alinéa 4 rappelle que pour les aspects de la relation de travail du Préposé qui ne sont pas directement réglés dans le présent projet la loi sur le personnel de l'Etat de Vaud (LPers) est applicable. Cela concerne notamment, le chapitre IV *Droits des collaborateurs*. | *Avis général : favorable avec une modification importante*<br><br>Pour assurer son indépendance, le Préposé doit être désigné par le Grand Conseil. Ceci serait également plus conforme aux exigences découlant de l'art. 15 par. 5 Convention 108+. |
| **Art. 33 Activités accessoires** | *Avis général : favorable* |

| Commentaire | Remarques (consultation) |
|---|---|
| Actuellement les règles applicables au Préposé en matière d'activité accessoires sont celles de la LPers. (art. 51). Cette disposition prévoit que l'autorité d'engagement soit informée par le collaborateur ou la collaboratrice et instaure un droit pour le Conseil d'Etat d'interdire l'exercice d'une activité incompatible avec la fonction.<br>L'art. 33 vient renforcer les exigences en matière d'exercice d'une activité accessoire par le Préposé. En effet, en application de l'art. 42 par. 3 de la directive (UE) 2016/680, le Préposé ne doit exercer aucune activité professionnelle incompatible qu'elle soit rémunérée ou non (à noter que cette disposition ne s'applique qu'au Préposé, le personnel de l'Autorité étant soumis à la règle générale de la loi sur le personnel de l'Etat de Vaud).<br>Al. 1, l'exercice d'une activité accessoire par le Préposé est, par principe, incompatible avec la nature de son activité mais également avec la garantie de son indépendance, que cette activité soit lucrative ou non. La deuxième phrase de cet alinéa vient compléter la disposition pour régler également l'exercice d'une fonction au sein d'un service de la Confédération, du canton ou d'une commune. Comme le mentionne le message du Conseil fédéral relatif à la LPD, cf. commentaire art. 41 *Activité accessoire* p. 6704, la notion de canton, communes comprises, doit être interprétée dans un sens large, à savoir qu'elle vise également les districts, cercles et corporation de droit public. Cette seconde phrase prescrit en outre que le Préposé ne peut pas non plus être membre de la direction, du conseil d'administration, de l'organe de surveillance ou de l'organe de révision d'une entreprise commerciale, ceci à nouveau indépendamment de la question de savoir si son activité est rémunérée ou non.<br>L'al. 2, également repris des art. 46 et 47 LPD, limite la portée de l'alinéa 1 en prévoyant un système d'autorisation par le Conseil d'Etat à certaines conditions. On pense, notamment, à une autorisation délivrée en vue de participer comme formateur dans un cursus privé dédié à la protection des données ou au droit à l'information. Pour le surplus, les dispositions idoines de la LPers et de son règlement d'application règlent la matière, notamment celles relatives au gain réalisé. | |
| **Art. 34 Fin anticipée des rapports de travail**<br><br>L'art. 34 régit les situations dans lesquelles les rapports de travail avec le Préposé peuvent prendre fin de manière anticipée. Ces règles correspondent à celles que prévoit l'art. 44 al. 2 et 3 LPD sur le plan fédéral. | *Avis général : favorable avec une modification importante*<br><br>La compétence de révoquer le Préposé doit revenir au Grand Conseil. C'est son indépendance qui en dépend. Le commentaire est trompeur à cet égard, car au niveau fédéral c'est bien le Parlement qui a cette compétence et pas le Conseil fédéral. |
| **Art. 35 Collaborateurs de l'Autorité** | *Avis général : favorable* |

| Commentaire | Remarques (consultation) |
|---|---|
| Al. 1 : gage de l'indépendance organisationnelle, l'engagement du personnel de l'Autorité par le Préposé prévu dans cette disposition reprend la teneur de l'art. 43 al. 5 deuxième phrase de la LPD. Le Préposé doit pouvoir organiser librement le recrutement et la gestion de ses ressources humaines – sous réserve bien évidemment des ressources financières disponibles - selon le plan organisationnel qu'il s'est fixé pour accomplir ses tâches et selon ses priorités. Il apparaît opportun que le Préposé soit l'autorité d'engagement de son personnel.<br>L'al. 2 rappelle que les collaboratrices et collaborateurs de l'Autorité est soumis à la LPers en leur qualité de personnel de l'Administration vaudoise. | |
| **Art. 36 Indépendance et organisation**<br><br>Comme commenté à l'article précédent, le projet prévoit de clarifier l'organisation de l'Autorité afin de poser le cadre de son indépendance.<br>L'al. 1 concrétise le principe d'indépendance de l'Autorité, conformément aux exigences de l'art. 15 par. 5 de la Convention 108+ et de l'art. 42 par. 1 et 2 de la directive (UE) 2016/680.<br>L'al. 2 propose, comme cela se fait au niveau de la Confédération (cf. art. 43 al. 5 LPD), de prévoir explicitement que l'Autorité dispose d'un budget propre, sachant que tel est déjà le cas actuellement, puisque l'APDI a un budget dévolu aux besoins de l'entité qui, une fois arrêté, vient s'intégrer au budget de la Chancellerie pour figurer au budget global de l'Etat. | *Avis général : favorable avec une observation*<br><br>L'al. 2 pourrait être plus clair sur la manière dont le budget est proposé et adopté, toujours dans le but de respecter l'indépendance. |
| **Art. 37 Rattachement**<br><br>L'autorité en charge de la protection des données et du droit à l'information a toujours été rattachée administrativement à la Chancellerie d'Etat. Ce rattachement permet de faire le lien entre l'Autorité et l'Etat notamment pour les questions budgétaires mais également pour tout ce qui touche aux ressources humaines, au support technique, ou à la commande de matériel, par exemple. Un tel rattachement administratif ne limite bien sûr en rien l'indépendance de l'APDI dans ses activités de protection des données (pour mémoire, le droit fédéral en la matière prévoit également un rattachement administratif du PFPDT à la Chancellerie fédérale). | *Avis général : favorable avec une observation*<br><br>Indépendamment du rattachement, il est répété ici que le Préposé ou la Préposée doit être désigné par le Grand conseil et non le Conseil d'Etat. |
| **Art. 38 Traitement des données par l'Autorité**<br><br>Conformément aux dispositions du présent projet, il appartient également à l'Autorité de se doter des bases légales nécessaires aux traitements des données qu'elle effectue en qualité de responsable du traitement.<br>L'al. 1 pose le cadre légal nécessaire au traitement en lien avec l'accomplissement des tâches de l'Autorité et prévoit également le traitement de données sensibles.<br>L'al. 2 fixe le principe de l'exploitation d'un système de gestion électronique des dossiers propre à l'Autorité. | |

| Commentaire | Remarques (consultation) |
|---|---|
| L'al. 3 prévoit que le règlement d'application de la LPrD fixe les dispositions d'exécution des traitements effectués par l'Autorité et énumère les points qui devront figurer dans le règlement, à savoir, les catégories de données personnelles traitées, les droits d'accès, les mesures de sécurité techniques et organisationnelles, les délais de conservation des données, leur archivage et leur effacement. | |
| **Art. 39 Autocontrôle de l'Autorité**<br><br>Al. 1, en qualité d'autorité administrative, l'Autorité est soumise à la LPrD au même titre que les entités visées à l'art. 2 al. 1 pLPrD. Dès lors se pose la question de sa surveillance dès lors qu'elle traite des données personnelles (responsable du traitement). Le droit fédéral a résolu la situation en prévoyant, cf. art. 48 LPD, une obligation pour le PFPDT de s'assurer, par des mesures de contrôle appropriées portant notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions fédérales de protection des données en son sein. Le présent projet propose de reprendre cette solution. En effet, une procédure d'autocontrôle dirigée par l'Autorité elle-même paraît plus opportune que la création un nouvel organe de surveillance qui devrait avoir les compétences nécessaires en la matière. On rappellera, par ailleurs, que cette procédure d'autocontrôle vient compléter les contrôles qui peuvent déjà être effectués par la Commission de gestion du Grand Conseil, par le Contrôle cantonal des finances ou par la Cour des comptes.<br>L'al. 2 charge l'Autorité de décrire, dans son rapport annuel, les mesures d'autocontrôle qu'elle a réalisées durant l'année écoulée. Cette façon de procéder est conforme au droit et vient renforcer la garantie du processus d'autocontrôle de l'Autorité. | |
| **Chapitre VI Tâches et pouvoirs de l'Autorité et des spécialistes en charge de la protection des données personnelles** | |
| **Introduction générale**<br><br>Le chapitre VI définit les tâches et pouvoirs de l'Autorité. En particulier, il confie à cette dernière la possibilité d'ouvrir des enquêtes (art. 40 p-LPrD), qui, si elles mettent en évidence des violations de dispositions de protection des données, pourront aboutir au prononcé de mesures administratives contraignantes (art. 42 p-LPrD). Ce pouvoir de décision accordé à l'Autorité constitue un renforcement notable de ses compétences puisque, dans la loi actuelle, le Préposé à la protection des données dispose seulement de la possibilité de formuler des recommandations, charge à l'Autorité de recourir au Tribunal cantonal si l'entité concernée refuse de les appliquer (cf. art. 36 LPrD).<br><br>Comme c'est le cas sur le plan fédéral (voir art. 49 LPD), l'art. 40 LPrD prévoit que, pour ouvrir une enquête, l'Autorité doit disposer d'indices suffisants de violation de la protection des données. Afin de compléter ce dispositif, en permettant à l'Autorité d'exercer une forme de surveillance indépendamment de l'existence de soupçons, l'art. 47 LPrD lui donne la faculté de réaliser des audits de traitements de données. L'objectif de ces audits sera de sensibiliser les entités concernées aux questions de protection des données et de les amener à améliorer leurs pratiques. | |

| Commentaire | Remarques (consultation) |
|---|---|
| D'autres tâches essentielles de l'Autorité consisteront notamment à renseigner les administré·e·s et les autorités au sujet des exigences et des droits prévus par le p-LPrD (art. 44 al. 1 let. b et c), ainsi qu'à prendre position sur les projets de règlementations impliquant le traitement de données personnelles (art. 44 let. d p-LPrD). Le chapitre VI règle encore la collaboration de l'Autorité avec ses homologues chargées de la protection des données, sur les plans fédéral, cantonal et communal (art. 45 p-LPrD), ainsi qu'en matière internationale (art. 46 p-LPrD). Enfin, il charge l'Autorité de publier un rapport annuel décrivant son activité (art. 48 p-LPrD). | |
| **Art. 40 Enquête**<br><br>Les conditions d'ouverture d'une enquête sont définies à l'alinéa 1. Celui-ci indique d'abord que l'Autorité peut agir d'office. Elle n'a donc pas besoin de recevoir une dénonciation pour intervenir. Cela étant, de la même manière qu'en droit fédéral, (art. 49 al. 1 LPD), l'Autorité doit disposer d'indices suffisants, laissant penser qu'un traitement de données pourrait violer une ou plusieurs dispositions de protection des données. En effet, dans la mesure où la procédure d'enquête confère à l'Autorité des pouvoirs d'instruction et de décision particulièrement étendus (art. 40 al. 4, art. 41, art. 42 pLPrD) et que la participation à l'enquête est susceptible de solliciter fortement les ressources de l'entité visée, il se justifie de limiter ces interventions aux cas dans lesquels il existe des raisons de penser que la loi a été violée (étant souligné qu'en l'absence de soupçons, l'Autorité aura la faculté de réaliser des audits selon l'art. 46 pLPrD). Il apparaît cependant opportun que les enquêtes qui seront ouvertes portent sur des affaires dans lesquelles les intérêts publics ou privés en jeu sont significatifs. C'est l'Autorité avant tout qui appréciera si une situation remplit ces conditions, cf. al. 2, dès lors qu'elle pourra renoncer à ouvrir une procédure dans les cas de peu d'importance. Pour ce faire, elle pourra se fonder sur plusieurs critères, notamment ceux exposés par la doctrine relative à l'art. 49 al. 2 LPD (permettant au Préposé fédéral à la protection des données de ne pas ouvrir d'enquêtes dans les cas de peu d'importance). Seront ainsi pris en compte, par exemple : La nature des données en question (sensibles ou non), le domaine du droit concerné (notamment le fait que le traitement de données litigieux soit éventuellement régi par la directive (UE) 2016/680), le nombre de personnes touchées, les mesures correctives déjà prises, le risque que la violation en question se reproduise, etc.<br>L'alinéa 3 indique que le responsable du traitement visé par une enquête doit en être informé. L'Autorité fournira cette information par écrit. Cette communication marquera l'ouverture de l'enquête. L'Autorité y précisera quels sont les traitements de données objets de l'enquête (soit ceux à propos desquels elle dispose d'indices suffisants d'une possible violation de la législation, conformément à l'alinéa 1).<br>L'alinéa 4 oblige le responsable du traitement, ainsi que des tiers, par exemple des sous-traitants, à concourir à l'enquête ouverte par l'Autorité. Il précise que ces personnes ne peuvent invoquer le secret de fonction pour refuser de répondre, à l'exception du secret fiscal, qui reste protégé, conformément à l'art. 157 de la loi du 4 juillet 2000 sur les impôts directs cantonaux. Un droit de refuser de collaborer dans certaines situations particulières leur est | *Avis général : favorable avec des modifications*<br><br>Dans l'ensemble, il est très positif d'octroyer au Préposé des pouvoirs d'enquête, à l'image de ce qui se retrouve également au niveau fédéral.<br><br>al. 4 un traitement différent pour le secret fiscal n'est pas justifié et doit être supprimé.<br><br>Al. 5 : l'Autorité **doit** l'informer (et non « peut ») |

| Commentaire | Remarques (consultation) |
|---|---|
| néanmoins reconnu, au travers d'un renvoi à deux dispositions du Code de procédure civile (CPC ; RS 272), les art. 160 al. 1 let. b et 166 al. 1 et 2 CPC. Il s'agit par exemple de permettre à une personne de refuser de répondre si cela risquerait de l'exposer ou d'exposer un de ses proches à une poursuite pénale ou d'engager leur responsabilité civile (voir art. 166 al. 1 let. a CPC), ou si les faits sur lesquels porte la question de l'Autorité sont protégés par le secret professionnel au sens de l'art. 321 du Code pénal (CP) (voir art. 166 al. 1 let. b CPC), etc. Pour la bonne clarté, il importe de souligner que dans l'enquête fondée sur les art. 40 et ss pLPrD, les restrictions prévues par l'art. 166 al. 1 et 2 CPC pourront être invoquées à la fois par les tiers et par le responsable du traitement lui-même (contrairement à ce que pourrait laisser entendre la phrase introductive de l'art. 166 al. 1 CPC qui, en procédure civile, ne vise que les « tiers » au procès). Sur le plan fédéral, l'art. 49 al. 3 LPD fixe des restrictions semblables aux pouvoirs d'investigation du PFPDT, en renvoyant aux art. 16 et 17 de la loi du 20 décembre 1968 sur la procédure administrative (PA ; RS 172.021).<br>L'alinéa 5 prévoit que l'Autorité puisse informer le dénonciateur de l'issue de l'enquête ouverte à la suite de son signalement. En revanche, comme l'indique l'alinéa 6, ce dénonciateur, ou d'autres personnes concernées, ne seront pas des parties à la procédure d'enquête, seul le responsable du traitement disposant d'un tel statut. Cette règle est similaire à celle que prévoit l'art. 52 al. 2 LPD sur le plan fédéral. Elle permet notamment d'assurer la célérité de l'enquête et d'éviter que cette procédure de surveillance soit employée avant tout pour servir des intérêts particuliers. Il sied de rappeler que les personnes qui souhaitent exercer des prétentions à l'encontre d'un responsable du traitement disposeront de tous les droits individuels prévus aux art. 26 et ss pLPrD. | |
| **Art. 41 Pouvoirs**<br><br>L'art. 41 al. 1 pLPrD correspond à l'art. 50 al. 1 LPD. Il permet à l'Autorité, si le responsable du traitement ou un tiers ne respecte pas l'obligation de collaborer qui lui incombe en vertu de l'art. 40 pLPrD, d'ordonner différentes mesures d'instructions contraignantes. Si nécessaire, cet ordre pourra aussi être assorti de la menace des peines prévues à l'art. 292 CP. Comme sur le plan fédéral, ce caractère graduel du pouvoir de contrainte de l'Autorité (en premier lieu, demande de renseignements et de documents selon l'art. 39 al. 2 pLPrD, puis, en cas de refus, décision ordonnant les mesures d'instruction prévues à l'art. 41 al. 1 pLPrD, éventuellement sous la menace d'une sanction pénale) traduit le principe de proportionnalité. Ainsi que l'indique l'emploi de l'adverbe « notamment » dans la phrase introductive, les mesures d'instruction citées à l'alinéa 1 ne sont pas exhaustives. Si elle l'estime nécessaire, l'Autorité pourra donc recourir à d'autres moyens d'investigation.<br>L'alinéa 2 reprend les limitations au devoir de collaborer prévues par l'art. 40 al. 3 pLPrD, qui restent logiquement applicables. Il est donc renvoyé au commentaire de cette disposition. | *Avis général : favorable avec des modifications*<br><br>Al. 2 : un traitement différent pour le secret fiscal n'est pas justifié et doit être supprimé.<br><br>Al. 3 : les mesures provisionnelles ne doivent pas être limitées aux domaines qui relèvent de la directive. Cela est déjà prévu à l'art. 86 LPA-VD.<br><br>Ajouter que l'Autorité peut faire appel aux organes de police cantonaux et communaux au besoin (cf. art. 50 al. 3 LPD) |
| **Art. 42 Mesures administratives** | *Avis général : favorable avec une suppression* |

| Commentaire | Remarques (consultation) |
|---|---|
| L'art. 42 pLPrD donne à l'Autorité le pouvoir d'ordonner des mesures administratives contraignantes si, à l'issue de l'enquête, elle constate que des dispositions de protection des données ont bien été violées. Cette disposition consacre un renforcement important des pouvoirs de l'Autorité, puisque dans la LPrD actuelle, elle dispose seulement de la compétence d'émettre des recommandations, que les entités concernées sont libres de suivre ou non (cf. art. 36 al. 4 LPrD). En cas de refus de leur part, c'est à l'Autorité qu'il incombe de recourir au Tribunal cantonal (cf. art. 36 al. 5 LPrD). Cette modification est notamment due aux exigences nouvelles prévues par la révision de la Convention pour la protection des personnes à l'égard des traitements de données personnelles du 18 mai 2018 (Convention 108+), ratifiée par la Suisse au mois de septembre 2023. La Confédération ainsi que la très grande majorité des cantons qui ont révisé leurs lois sur la protection des données récemment ont ainsi accordé un pouvoir de décision aux autorités de surveillance que ces lois désignent.<br>Les mesures qui peuvent être ordonnées sont définies de façon exhaustive par l'alinéa 1. Il est possible de les classer en deux catégories. La première comprend les mesures qui visent à régler des problèmes de conformité à des exigences spécifiques de la pLPrD, soit essentiellement celles qui imposent un devoir d'information au responsable du traitement. Il s'agit des cas prévus aux lettres a et d, qui permettront de remédier, par exemple, à la violation de l'obligation d'informer une personne qu'elle a fait l'objet d'une décision individuelle automatisée, ou à la violation de l'obligation d'annoncer un traitement au registre des activités de traitement. La deuxième catégorie comprend des mesures plus générales, qui pourront s'appliquer à une multitude de situations. Il s'agit des cas prévus par les lettres e à g. D'une part, l'Autorité pourra ordonner la rectification, la suppression ou la destruction de données personnelles qui auraient été collectées ou conservées de façon contraire au droit (art. 42 al. 1 let. b pLPrD). D'autre part, lorsqu'elle constate qu'une situation pose des problèmes de conformité au droit, l'Autorité pourra impartir au responsable du traitement un délai approprié pour y remédier (art. 42 al. 1 let. d pLPrD). Ce délai sera fixé dans le respect des exigences du principe de proportionnalité. Cela n'exclut pas qu'il soit extrêmement bref, si les circonstances rendent nécessaires une réaction urgente. En même temps qu'elle impose ce délai, l'Autorité pourra évidemment suggérer les mesures correctives qu'elle estime indiquées. Du reste, un soutien de sa part sera certainement attendu par des responsables du traitement. Cela dit, conformément au principe de la séparation des pouvoirs, la pLPrD laisse toujours au responsable du traitement le choix des mesures à prendre.<br>En dernier lieu, si le responsable du traitement refuse d'agir, ou s'il prend des mesures jugées insuffisantes, et qu'elle n'entend pas impartir un nouveau délai, l'Autorité pourra ordonner la suspension ou la cessation pure et simple d'un traitement de données, ou d'une partie d'un traitement de données, jusqu'à-ce que celui-ci soit mis en conformité (art. 42 al. 1 let. g pLPrD).<br>L'alinéa 2 prévoit que les entités concernées peuvent recourir au Tribunal cantonal contre les décisions de l'Autorité. Enfin, l'alinéa 3 reprend la règle qui figure actuellement à l'art. 13 al. 2 LPrDS et permet à l'Autorité | L'al. 3 reprend exactement l'al. 3 de l'art. 41 et doit être supprimé |

| Commentaire | Remarques (consultation) |
|---|---|
| d'ordonner des mesures provisionnelles pendant la durée de l'enquête, lorsque les traitements de données concernés relèvent de la Directive Schengen. | |
| **Art. 43 Application de la procédure administrative vaudoise**<br><br>L'art. 43 al. 1 pLPrD prévoit que les décisions rendues par l'Autorité au cours de la procédure d'enquête peuvent faire l'objet d'un recours au Tribunal cantonal de la part du responsable du traitement (lequel se voit ainsi reconnaître la qualité pour recourir par la loi, ce qui correspond à l'éventualité prévue par l'art. 75 al. 2 de la loi du 28 octobre 2008 sur la procédure administrative [LPA-VD ; BLV 173.36], applicable au recours de droit administratif en vertu de l'art. 99 LPA-VD).<br>Au surplus, l'art. 43 al. 2 pLPrD déclare la LPA-VD applicable à la procédure d'enquête pour tous les aspects que la pLPrD ne règle pas expressément. Ce renvoi à la LPA-VD concerne aussi la procédure de recours. Cela signifie notamment que l'art. 74 LPA-VD définira si une décision incidente de l'Autorité peut faire l'objet d'un recours immédiat de la part du responsable du traitement, ou si elle ne peut être contestée que dans le cadre du recours contre la décision finale. Ce sont aussi les règles ordinaires de la LPA-VD qui régiront le droit de recourir de tiers qui seraient touchés par des décisions de l'Autorité (soit avant tout des ordres de production de pièces ou d'autres mesures d'instruction ordonnées en vertu de l'art. 41 pLPrD). | *Avis général : favorable avec modification*<br><br>Il faut aussi ajouter que l'Autorité a qualité de partie et peut recourir contre les décisions, y compris sur recours, rendues en application des art. 42 et 52. |
| **Art. 44 Autres tâches**<br><br>L'art. 44 pLPrD décrit les autres tâches confiées à l'Autorité. Dans une très large mesure, cette disposition correspond à l'art. 37 LPrD actuel. L'Autorité est d'abord chargée de promouvoir, de manière générale, la protection des données au niveau cantonal (let. a). Cela peut inclure, par exemple, l'organisation de manifestations ou de campagnes de communication à but informatif, ainsi que celle de formations continues, notamment pour les responsables du traitement. Une mission particulièrement importante de l'Autorité sera de renseigner et conseiller les responsables de traitement sur les exigences posées en matière de protection des données (let. b). Ces responsables du traitement, par exemple des autorités communales, pourront ainsi s'adresser à l'Autorité pour obtenir conseil et soutien, lorsque des questions de protection des données se présenteront à eux. L'autorité sera aussi chargée de renseigner les personnes concernées par un traitement de données sur les droits que la pLPrD leur confère (let. c). En d'autres termes, elle pourra expliquer à ces personnes la teneur des droits prévus par les art. 26 et ss pLPrD et leur fournir des conseils quant aux moyens appropriés de faire valoir ces droits. L'Autorité devra aussi être consultée chaque fois qu'un projet législatif émanant d'une entité soumise à la LPrD selon l'art. 2 al. 1 pLPrD implique le traitement de données personnelles (let. d). L'Autorité a encore pour tâche de gérer le Registre | *Avis général : défavorable quant à la disparition des tâches de conciliation et d'autorité de recours*<br><br>Vu le modèle retenu, il n'y a plus de possibilité de conciliation ni de recours devant l'Autorité. Toute personne concernée devra donc directement recourir à la CDAP. Si la procédure est gratuite, ce choix va augmenter très sensiblement le nombre de recours devant la CDAP, ce qui représente une charge pour cette dernière et les entités.<br><br>Il serait préférable de choisir un modèle largement partagé dans les cantons latins avec un Préposé qui conseille, surveille, concilie et instruit, et émet des recommandations, et une autorité ou commission qui rend des décisions. |

| Commentaire | Remarques (consultation) |
|---|---|
| des activités de traitement (let. e). Enfin, l'Autorité collaborera avec ses homologues suisses et étrangères, étant précisé que les modalités de cette coopération sont précisées aux art. 45 et 46 pLPrD (let. f). | Par ailleurs, la compétence de conseiller puis rendre une décision contraignante dans le même domaine (surveillance) n'est pas cohérente et rend le travail du Préposé incohérant.<br><br>Une tâche de surveillance générale doit être ajoutée. Le Préposé doit aussi avoir la possibilité de demander des informations pour évaluer la conformité d'un traitement (surveillance) en l'absence de soupçon. Cette phase préalable doit permettre aussi de décider ou non d'ouvrir une enquête. |

**Art. 45 Coopération avec d'autres autorités de protection des données en Suisse**

**Art. 46 Coopération avec d'autres autorités de protection des données à l'étranger**

Ces dispositions fixent les règles à suivre lorsque l'Autorité est amenée à coopérer avec d'autres autorités de protection des données, en Suisse ou à l'étranger et à échanger dans ce cadre des données personnelles, y compris des données personnelles sensibles.

Sur le plan interne à la Suisse, l'Autorité pourra communiquer des informations avec les autres autorités fédérale et cantonales si les conditions de l'art. 45 al. 2 pLPrD sont remplies, soit si cette communication est indispensable à l'accomplissement des tâches qui leur incombent. Les principes généraux de protection des données (spécialité, proportionnalité, qui interdit les requêtes exploratoires non-ciblées [« *fishing explorations* »]) demeurent bien sûr applicables et encadreront ces échanges.

L'art. 46 al. 1 pLPrD soumet la collaboration avec des autorités étrangères à des exigences accrues, destinées à garantie la protection des données qui seront transmises. Ces conditions correspondent à celles prévues par l'art. 55 al. 1 LPD sur le plan fédéral. Selon la première (let. a), le principe de réciprocité en matière d'assistance administrative dans le domaine de la protection des données doit être garanti entre la Suisse et l'Etat étranger. Deuxièmement, conformément au principe de spécialité, les informations et les données personnelles échangées ne doivent être utilisées que dans le cadre de la procédure liée à la protection des données à la base de la demande d'assistance (let. b). Si les données transmises doivent être utilisées ultérieurement dans le cadre d'une procédure pénale, les dispositions sur l'entraide judiciaire internationale en matière pénale s'appliquent. Les troisième et quatrième conditions garantissent le respect des secrets professionnels, d'affaires et de fabrication (let. c) et interdisent que les informations et les données échangées soient communiquées à des tiers sans l'accord préalable de l'autorité qui les a transmises (let. d). Enfin, l'autorité destinataire doit respecter les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations (let. e).

Enfin, l'art. 46 al. 2 pLPrD correspond à l'art. 55 al. 3 LPD. Lorsque, dans le cadre d'une procédure d'assistance administrative, le préposé envisage de transmettre à une autorité étrangère chargée de la protection des données des informations susceptibles de contenir des secrets professionnels ou des secrets d'affaires ou de fabrication, il est tenu d'informer les personnes concernées en les invitant à prendre position. Le préposé est néanmoins délié de son obligation si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.

| Commentaire | Remarques (consultation) |
|---|---|
| **Art. 47 Audit**<br><br>Sur la base de la LPrD actuelle, l'Autorité procède à des audits de protection des données, notamment dans le domaine de la vidéosurveillance. Cela signifie qu'elle se charge, ou charge un tiers, d'examiner la pratique d'une autorité au regard de la législation en matière de protection des données, avant de publier un rapport exposant ses constats. Cependant, la loi ne définit guère le cadre juridique de ces audits, respectivement le distingue mal de celui de l'enquête. Ainsi, le terme d'« audit » ne figure qu'à l'art. 36 al. 6 LPrD, lequel ne précise ni dans quels cas, ni à quelles fins, ni selon quelle procédure ces audits sont menés. Ceci est problématique, notamment parce qu'un rapport d'audit est susceptible de se montrer très critique à l'égard d'une autorité, par exemple une commune, sans que celle-ci n'ait de moyens de réclamer la correction d'éléments qu'elle juge erronés, la procédure de l'art. 36 al. 3 à 5 LPrD n'étant pas applicable. Le Conseil d'Etat entend donc profiter de la présente révision de la loi sur la protection des données pour définir de façon plus claire la procédure d'audit et mieux établir ses différences d'avec la procédure d'enquête, étant souligné que ce sont ces différences qui justifient de conserver cette institution, que d'autres lois sur la protection des données (dont la LPD) ne connaissent pas, parmi les mesures de surveillance à disposition de l'Autorité.<br>L'alinéa 1 définit les conditions dans lesquelles l'Autorité peut réaliser un audit et les finalités de cette démarche. Contrairement à l'ouverture d'une enquête (cf. art. 40 al. 1 pLPrD), le lancement d'un audit ne nécessite pas d'indices de violation de dispositions de protection des données. En d'autres termes, l'Autorité pourra décider d'auditer spontanément un responsable du traitement. Ceci s'explique par le fait que le but de l'audit n'est pas de chercher à corroborer des soupçons quant à la licéité des traitements de données concernés, mais de sensibiliser le responsable du traitement aux exigences de la protection des données et le cas échéant, de lui proposer des améliorations de sa pratique. Cette finalité différente de l'enquête explique aussi pourquoi la procédure d'audit ne prévoit pas les mêmes obligations de collaboration du responsable du traitement et des tiers ni les mêmes pouvoirs contraignants de l'Autorité que les art. 40 à 42 pLPrD. Cela étant, si un audit met en lumière des indices suffisants de violation importantes de dispositions de protection des données, au sens de l'art. 40 al. 1 pLPrD, l'Autorité pourra décider d'ouvrir une procédure d'enquête et disposera alors de tous les pouvoirs liés à ce type d'intervention.<br>L'alinéa 2 indique que l'Autorité doit indiquer au responsable du traitement concerné sur quoi portera l'audit. Cette information doit intervenir avant le début de l'audit. L'alinéa 3 permet à l'Autorité de confier la réalisation des audits à des tiers prestataires, comme elle le fait déjà aujourd'hui.<br>L'alinéa 4 reprend l'art. 36 al. 6 LPrD actuel, en lui apportant la précision selon laquelle les rapports d'audits ne sont pas rendus publics. La procédure d'audit se conçoit comme un moyen d'améliorer les pratiques, non comme une démarche coercitive. Dans cette optique, il importe que le responsable du traitement audité ait la liberté d'examiner s'il doit modifier sa façon de travailler, sans être soumis à des pressions publiques ou médiatiques | *Avis général : défavorable avec suppresssion*<br><br>Cet article doit être supprimé car il complique inutilement la procédure.<br>En cas de soupçons, une enquête doit être ouverte. En l'absence de soupçons, l'Autorité peut déjà conseiller les entités et une compétence de surveillance doit être ajoutée à l'art. 44.<br>L'activité de surveillance peut déboucher sur un conseil ou une enquête, mais cela ne doit pas être une activité d'audit séparée, avec des rapports non publics mais largement diffusés et menés par des tiers.<br>L'Autorité doit toujours pouvoir s'appuyer sur un mandat externe lorsque cela est nécessaire, mais la loi ne doit pas prévoir que les rapports d'audits sont délégables à des tiers.<br>De plus, la Cour des comptes a également des compétences de surveillance. |

| Commentaire | Remarques (consultation) |
|---|---|
| importantes, qui ne manqueraient pas de s'exercer si des observations critiques étaient largement diffusées. Ceci apparaît d'autant plus opportun que, comme aujourd'hui, les rapports d'audits ne pourront pas faire l'objet de recours, au travers desquels le responsable du traitement pourrait demander à un juge de corriger des conclusions inexactes de l'auditeur. Par cette visée « interne », les audits de l'art. 47 pLPrD se rapprocheront de ceux réalisés par le Contrôle cantonal des finances, qui ne sont pas non plus rendus publics, sauf si le Conseil d'Etat le décide (voir art. 17 et 18 de la loi du 12 mars 2013 sur le Contrôle cantonal des finances ; BLV 614.11). Cela étant, selon l'art. 47 al. 4 pLPrD, le rapport d'audit sera aussi communiqué à l'autorité dont dépend hiérarchiquement le responsable du traitement. Celle-ci pourra donc veiller à ce que l'audit soit bien pris en compte, respectivement demander des explications au responsable du traitement, s'il n'entend pas modifier sa pratique. Les deux autres destinataires du rapport d'audit (Présidences du Conseil d'Etat et de la Commission de gestion du Grand Conseil) sont ceux que désigne déjà l'art. 36 al. 6 LPrD. | |
| **Art. 48 Rapport annuel**<br><br>L'art. 48 correspond à l'art. 57 LPD sur le plan fédéral et demande à l'Autorité d'établir un rapport annuel d'activité. L'autorité pourra notamment y mentionner les décisions qu'elle aura rendues à la suite d'enquêtes (en revanche, compte-tenu du caractère non-public des audits au sens de l'art. 47 pLPrD, le rapport annuel ne fournira pas des indications détaillées sur ces audits). | *Avis général : favorable avec observation et modification*<br><br>À l'alinéa 2, il est prévu que : « Elle présente son rapport au Conseil d'État et au Grand Conseil en mai de chaque année ». Le GC étant l'autorité suprême du canton, ce rapport ne devrait être présenté qu'à celui-ci, d'autant plus si le Préposé est désigné par le GC. Il est étrange de présenter un rapport à 2 autorités différentes. A titre d'exemple, le rapport de la médiatrice cantonale est soumis et examiné par le Grand Conseil. Dans le cadre de cet article, un rapport pourrait lui être effectivement soumis tout en s'interrogeant sur l'éventuel organe parlementaire qui l'examinerait en amont. Par exemple, la Commission thématique des affaires juridiques (CTAFJ) examine le rapport annuel du Conseil de la magistrature (CM). Il faut s'interroger si ce rapport est un rapport d'information à destination du Grand Conseil ou s'il doit être examiné en amont par une commission parlementaire. |

| Commentaire | Remarques (consultation) |
|---|---|
| **Chapitre VII Registre des activités de traitement**<br><br>Le registre des fichiers devient le registre des activités de traitement. Ainsi, l'obligation de déclarer les activités de traitement remplace l'obligation de déclarer les fichiers qui figure dans le droit en vigueur. L'obligation de tenir un registre des activités de traitement découle de l'art. 24 de la directive (UE) 2016/680. Elle est reprise en droit fédéral à l'art. 12 LPD.<br>Le registre des activités de traitement est un élément essentiel de la mise en œuvre de la protection des données. Il constitue un outil indispensable de gouvernance et de documentation, qui assure à la fois la transparence et le contrôle des activités de traitement des organes publics. L'obligation d'annonce des activités de traitement dans le registre implique notamment que le responsable du traitement de données soit à même de déterminer, pour chaque traitement, qui traite des données, quelles sont les catégories de personnes concernées, quelles sont les données traitées, dans quel but, selon quelles modalités, qui a accès à ces données, combien de temps elles sont conservées, quelles mesures de sécurité ont été prises, etc.<br>Le déploiement du registre des fichiers accusant du retard, les communes et les délégataires de tâches publiques n'ont pour l'heure pas été en mesure d'annoncer leurs fichiers dans celui-ci. Il conviendra de remédier à la situation dans les meilleurs délais. Une période transitoire de cinq ans dès l'entrée en vigueur de la loi est prévue pour la mise en conformité au registre des activités de traitement (art. 56 al. 2 LPrD). S'agissant du Conseil d'Etat et son administration, du Grand Conseil et son administration ainsi que de l'Ordre judiciaire vaudois, qui ont déjà procédé à l'annonce de leurs fichiers, la mise à jour devra être réalisée dans un délai de 5 ans. | |
| **Art. 49 Registre des activités de traitement**<br><br>Selon l'al. 1, l'Autorité tient un registre des activités de traitement, qui est public et accessible via le site internet de l'Autorité. Concrètement, le registre est tenu par l'Autorité qui en assure le bon fonctionnement technique et la publicité. Le responsable du traitement ou les responsables conjoints du traitement restent en revanche seuls garants du contenu des annonces réalisées dans le registre. L'Autorité ne saurait ainsi être tenue responsable des informations publiées. Afin d'assurer la meilleure visibilité possible, le registre des activités de traitement est consultable sur le site Internet de l'Autorité. Pour les personnes qui disposeraient d'une accessibilité limitée aux technologies de l'information, une consultation avec un membre de l'APDI peut être organisée, voire une liste papier établie. Cela permet d'éviter la fracture numérique. | *Avis général : favorable avec modification*<br><br>C'est une obligation qui doit figurer dans le chapitre III<br><br>La solution vaudoise retient un registre cantonal dans lequel les entités doivent annoncer leurs activités. Au niveau fédéral, chaque responsable du traitement doit tenir son registre et les organes fédéraux les déclare au PFPDT qui les publie. |

| Commentaire | Remarques (consultation) |
|---|---|
| L'al. 2 précise les informations minimales que doit contenir le registre. L'identité et les coordonnées du responsable du traitement, la base légale fondant le traitement ainsi que les finalités du traitement doivent y être renseignées. Le registre doit également indiquer les personnes concernées ou les catégories de personnes concernées, les données personnelles ou les catégories de données personnelles traitées et les destinataires ou les catégories de destinataires des données personnelles si la communication des données personnelles est envisagée, y compris les destinataires dans des pays tiers ou des organisations internationales. Par catégories des personnes concernées on entend des groupes partageant les mêmes caractéristiques (« administré·e·s » ou « employé·e·s », par ex). On entend également par là des groupes partageant les mêmes caractéristiques (« autorités de surveillance », par ex.). Les catégories des données personnelles traitées désignent la nature des données (données sensibles, par ex.). En effet, en fonction des circonstances, il n'est parfois pas possible, au vu de pluralité de situations rencontrées, d'attendre d'un responsable du traitement qu'il décrive avec précision toutes les données traitées. Un tel descriptif pourrait au contraire donner à la plupart des personnes concernées l'impression que davantage de données les concernant sont traitées que ce n'est le cas en réalité. Le registre doit aussi indiquer la durée de conservation ou, si cela n'est pas possible, les critères pour déterminer cette durée. A noter que les durées de conservation avant élimination fixées par les calendriers de conservation ou les référentiels de conservation n'ont pas valeur de base légale, cf. arrêt de la CDAP du 5 avril 2022, GE.2020.0121, confirmé par arrêt du TF du 8 février 2023, 1C_273/2022. La durée étant liée, conformément à l'art. 6 LPrD aux finalités du traitement et devant faire l'objet d'une pesée d'intérêt sous l'angle de la proportionnalité, il n'est pas toujours possible de l'établir avec précision, d'où la mention « si cela n'est pas possible ». S'il n'est pas possible de fournir une indication précise, le registre doit au moins indiquer les critères selon lesquels ce délai sera fixé. Finalement, les mesures visant à garantir la sécurité des données doivent, dans la mesure du possible, être renseignées. Le but de cette description est de faire apparaître d'éventuels manquements dans les mesures de sécurité. La mention « dans la mesure du possible » indique que cette obligation ne s'applique que si les mesures peuvent être définies de manière suffisamment concrète et qu'elles ne mettent pas en péril la confidentialité des données en question. A noter que, comme cela était le cas s'agissant des informations figurant dans le registre des fichiers, cf. | |

| Commentaire | Remarques (consultation) |
|---|---|
| arrêt de CDAP du 3 juin 2020 GE.2019.0162, les informations figurant dans le registre des activités de traitement n'ont qu'une portée indicative.<br>Comme cela est déjà le cas en droit actuel, le Conseil d'Etat édictera les règles applicables à la tenue du registre (al. 3). | |
| **Art. 50 Annonce**<br><br>A l'instar de ce qui se fait à l'heure actuelle s'agissant du registre des fichiers, les entités soumises à la loi devront immédiatement annoncer leurs activités de traitement à l'Autorité par le biais du registre. Il est en effet dans l'intérêt des responsables du traitement et des personnes concernées que l'annonce soit réalisée le plus rapidement possible. | *Avis général : favorable avec possibilité de simplification*<br><br>L'art. 50 peut être remplacé par un simple alinéa à l'art. précédent qui indique que les entités déclarent leur registre. |
| **Art. 51 Exceptions**<br><br>L'art. 51 fixe un certain nombre d'exceptions à l'obligation de déclarer. La liste des exceptions est modifiée par rapport au droit actuel pour tenir compte de la pratique. | |
| **Chapitre VIII Voies de droit, procédure** | |

| Commentaire | Remarques (consultation) |
|---|---|
| **Art. 52 Décision du responsable du traitement**<br>**Art. 53 Recours**<br><br>Les art. 52 et 53 pLPrD règlent la procédure applicable lorsqu'un responsable du traitement refuse une demande fondée sur les art. 26 à 31 pLPrD.<br>Par rapport au système actuel (art. 30 à 33 LPrD), deux changements sont à noter. Le principal est que la pLPrD ne prévoit plus de voie de recours alternative à l'Autorité ou au Tribunal cantonal, comme le fait l'art. 31 al. 1 de la LPrD actuelle. Il a été constaté que cette double voie de recours n'apporte pas de plus-value notable en matière de protection des données. Au contraire, l'existence du recours devant l'Autorité complique la mission de cette dernière, consistant à fournir des renseignements aux personnes concernées, sur la façon d'exercer leurs droits auprès des responsables du traitement. Il est en effet difficile pour l'Autorité de prodiguer de tels conseils, alors que sa position d'autorité de recours commanderait qu'elle conserve une position neutre dans la procédure. Au demeurant, l'existence d'un recours alternatif à l'Autorité ou au Tribunal cantonal est une particularité vaudoise historique. Ni la Confédération, ni les autres cantons ne le prévoient.<br>L'autre modification consiste à prévoir, à l'art. 52 al. 2 pLPrD, que la décision du responsable du traitement refusant une demande fondée sur les art. 26 à 31 pLPrD ne sera communiquée à l'Autorité qu'à la demande de la personne concernée (alors qu'aujourd'hui cette notification est systématique, selon l'art. 30 al. 2 LPrD). Il est en effet concevable que la personne concernée ne souhaite pas que des tiers soient avisés de la procédure qu'il a entreprise devant un responsable du traitement. Cette adaptation va donc dans le sens d'un renforcement de la protection des données. | *Avis général : favorable avec modifications*<br><br>52 al. 2 la communication à l'Autorité devrait être systématique (le secret de fonction ne lui est pas opposable) et l'Autorité doit avoir un droit de recours. 53. Il faut préciser que la décision est sujette à recours au sens de la LPA-VD même si l'entité n'est, en dehors de la LPrD, pas compétence pour rendre une décision au sens de l'art. 3 LPA-VD. |
| **Chapitre IX Dispositions pénales** | |
| **Art. 54 Violation du devoir de discrétion**<br><br>L'art. 54 pLPrD prévoit les cas dans lesquels la révélation intentionnelle de données personnelles est punissable pénalement. L'art. p-54 LPrD habilite expressément l'Autorité à dénoncer aux autorités de poursuite pénales les faits susceptibles de constituer une infraction à l'art. 54 pLPrD.<br>**Art. 55 Dénonciation par l'Autorité** | *Avis général : favorable avec modifications et défavorable pour l'art. 55*<br><br>Préciser dans le commentaire que l'art. 54 est subsidiaire au secret de fonction. |

| Commentaire | | Remarques (consultation) |
|---|---|---|
| | | L'art. 55 est malheureux. S'il concerne la dénonciation d'infractions pénales en général, la situation ne doit pas être différentes pour le Préposé des autres fonctionnaires et cela ressort de la LPers.<br>Si cela vise seulement l'art. 54, il n'y a pas lieu de faire un art. séparé, ni de le traiter différemment du secret de fonction. |
| **Chapitre X Dispositions transitoires et finales** | | |
| **Art. 56 Abrogation** | | |
| **Art. 57 Dispositions transitoires** | | Al. 1 : les entités privées qui exercent une tâche publique ne peuvent pas adopter de législation.<br>Al. 4 il faut préciser que les mandats précédents compte au sens de l'art. 32. |
| **Art. 58 Disposition finale** | | |