



Rapport accompagnant

L'avant-projet de Loi sur la vidéosurveillance (LVid)

1. Table des matières

1.	Table des matières	1
2.	Origines du projet et fondements légaux	2
2.1.	Origines du projet	2
2.2.	Fondements légaux	2
3.	Considérations générales	5
3.1.	Notion	5
3.2.	Buts et intérêts en cause	6
3.3.	La situation réglementaire en Suisse	7
3.3.1.	Sur le plan fédéral	7
3.3.2.	Sur le plan cantonal	8
4.	Commentaire des dispositions	10
4.1.	Article 1	10
4.2.	Article 2	11
4.3.	Article 3	13
4.4.	Article 4	16
4.5.	Article 5	18
4.6.	Article 6	19
4.7.	Article 7	19
4.8.	Article 8	20
4.9.	Article 9	20
4.10.	Article 10	21
4.11.	Article 11	22
4.12.	Article 12	24
4.13.	Article 13	25
4.14.	Article 14	26
4.15.	Article 15	28
4.16.	Article 16	29
4.17.	Article 17	30
4.18.	Article 18	30
4.19.	Article 19	31
4.20.	Article 20	32
4.21.	Article 21	33
4.22.	Article 22	33
4.23.	Article 23	34
5.	Considérations finales	34

2. Origines du projet et fondements légaux

2.1. Origines du projet

Par décision du 5 février 2014 faisant suite à un rapport qui lui avait été présenté le 31 janvier précédent par le Chancelier d'État, le Conseil d'État du Canton du Valais a pris acte de la nécessité d'élaborer une base légale spécifique régissant la vidéosurveillance dans les lieux publics, les locaux administratifs ainsi que les bâtiments du gouvernement appartenant à l'État du Valais. Pour ce faire, il a institué un groupe de travail composé de la Vice-chancelière d'État (présidente), du Commandant de la Police cantonale, du Chef de service du Département de la Formation et de la Sécurité (DFS), du Chef de service du Service des affaires intérieures et communales (SAIC), de la Préposée à la protection des données du canton du Valais ainsi que d'un membre désigné par la Fédération des communes valaisannes. Suite à divers contretemps, l'entrée en fonction de la personne en charge du poste de Préposé à la protection des données du canton du Valais (le Préposé) n'est finalement intervenue qu'en automne 2014. Ce n'est dès lors qu'à ce moment que le groupe de travail a pu se pencher sur le projet de loi envisagé. Quatre moutures d'un premier projet de loi ont été élaborées, selon les avis et points de vue exprimés par ses membres. Sur requête du Groupe de travail, le Conseil d'État a nommé Dr Sylvain Métille en qualité d'expert le 16 novembre 2016 et lui a donné mandat de présenter un avant-projet de loi accompagné d'un rapport explicatif.

2.2. Fondements légaux

La liberté individuelle est garantie au niveau cantonal à l'article 4 alinéa 1 de la Constitution du Canton du Valais (« **Cst. VS** »)¹. Elle est notamment mise en œuvre, sous l'angle de la protection des données, par la Loi sur l'information du public, la protection des données et l'archivage (« **LIPDA** »)².

La LIPDA a pour but notamment de garantir à chacun le respect de ses droits et de ses libertés fondamentales lors du traitement de données à caractère personnel par les organes publics (art. 1 al. 2 let. b LIPDA). Elle ne s'applique en revanche pas au traitement de données personnelles par des personnes privées ou des organes fédéraux, qui est soumis à la Loi fédérale sur la protection des données et la transparence (« **LPD** »)³.

Les principes généraux applicables à tout traitement de données sont exprimés aux articles 17 ss LIPDA. Il s'agit en particulier des principes de légalité (art. 17 al. 1 et 3), de

¹ RS VS 101.1.

² RS VS 170.2.

³ RS 235.1.

proportionnalité (art. 17 al. 2), de finalité (art. 17 al. 2) et de sécurité des données (art. 21). Une obligation d'informer lors de la collecte de données personnelles (qui peut être limitée à certaines conditions) est également prévue aux articles 19 à 20 LIPDA.

La LIPDA contient en parallèle, à son article 28, une règle traitant spécifiquement de la surveillance des lieux publics par des appareils de prise de vues et d'enregistrement d'images. Il y est indiqué qu'une autorité peut, afin de contribuer à la sécurité des personnes et des biens, installer des appareils de prise de vues et d'enregistrement d'images sur le domaine public moyennant la réalisation de trois conditions :

- une loi au sens formel l'y autorise;
- les mesures nécessaires sont prises pour limiter les atteintes aux personnes concernées;
- et
- les informations enregistrées ne sont utilisées qu'aux fins fixées dans la loi qui institue le système de surveillance.

Ces mesures de surveillance ainsi que l'autorité responsable doivent être indiquées de manière claire et adéquate au public (al. 2) et la durée de conservation des données enregistrées, de même que les organes habilités à visionner les images, doivent être fixés dans la loi spéciale en fonction des besoins et objectifs (al. 3).

La LIPDA et son article 28 LIPDA en particulier ne sont pas une base légale formelle permettant de mettre en place un système de vidéosurveillance. Une loi formelle devrait être adoptée par chaque législatif cantonal et communal, de manière générale ou dans chaque cas d'espèce. Une telle solution est difficilement praticable et conduit en réalité à la présence de nombreuses caméras sans que la base légale nécessaire n'ait été adoptée.

La LVid doit dès lors combler cette lacune et servir de base légale générale au sens de l'article 28 alinéa 1 lettre a LIPDA. Comme elle s'applique à de nombreuses situations différentes, elle repose sur un système d'autorisation à même de prendre en compte les particularités de chaque situation, tant au niveau cantonal que communal. Elle respecte en outre l'autonomie des communes, tout en garantissant une uniformité des principes au niveau cantonal. Elle tient en outre compte des principes généraux de la LIPDA qui régissent toute forme de récolte et de traitement de données personnelles.

En parallèle à la LIPDA, la vidéosurveillance fait déjà l'objet d'autres dispositions légales dans les domaines policier et pénal.

Sur le plan fédéral, les articles 280 ss du Code de procédure pénale suisse (« **CPP** »)⁴ détaillent plusieurs mesures de surveillance secrètes qui peuvent être mises en œuvre par le ministère public dans le contexte d'une procédure pénale. L'article 280 lettre b CPP permet notamment d'observer ou d'enregistrer des actions se déroulant dans des lieux qui ne sont pas publics ou qui ne sont pas librement accessibles. L'article 282 alinéa 1 CPP prévoit pour sa part la possibilité d'observer secrètement des personnes et des choses dans des lieux librement accessibles et d'effectuer des enregistrements audio et vidéo. Des autorisations, respectivement du ministère public et du tribunal des mesures de contrainte sont requises. La personne concernée sera ensuite informée et pourra faire valoir ses droits sur la base du CPP. Au niveau cantonal, la Loi sur la police cantonale (« **LPol** »)⁵ a été modifiée le 11 novembre 2016.

Le nouvel article 42 LPol traite de l'observation préventive et permet à la police cantonale, afin d'empêcher la commission de crimes ou de délits, d'observer secrètement des personnes et des choses dans des lieux librement accessibles, y compris d'effectuer des enregistrements audio et vidéo. Cette surveillance a lieu avant l'ouverture d'une procédure pénale mais les dispositions sur la surveillance du CPP s'appliquent par analogie. Si la surveillance dépasse un mois, l'autorisation du ministère public est requise.

Conformément à la jurisprudence du Tribunal fédéral⁶, un canton peut prévoir des mesures de surveillance secrètes à des conditions similaires à celles prévues par le CPP. Pour observer ou enregistrer des actions se déroulant dans des lieux qui ne sont pas publics ou qui ne sont pas librement accessibles, un régime similaire à celui des article 280 ss CPP (autres mesures de surveillance) est nécessaire et implique une autorisation judiciaire.

Le nouvel article 58 LPol prévoit pour sa part que la police peut mettre en place une vidéosurveillance, ainsi qu'une audiosurveillance, dans l'espace public. Un tel système est prévu dans le but de suivre directement ce qui se passe en un lieu déterminé et permettre à la police cantonale d'intervenir rapidement et de manière appropriée (a); pour la régulation du trafic (b); lors de manifestations s'il y a de sérieuses raisons de présumer que des actes punissables pourraient être commis à l'encontre des personnes ou des objets (c) ; et pour la prévention d'un crime ou d'un délit lorsque les autres modes d'intervention paraissent insuffisants (d).

Enfin, l'article 59 LPol permet la recherche automatisée de véhicules et de personnes.

⁴ RS 312.0.

⁵ RS VS 550.1.

⁶ Notamment 1C_653/2012 et 1C_518/2013 du 1er octobre 2014.

L'adoption d'une ordonnance détaillant ces différentes hypothèses de vidéosurveillance, y compris pour les modalités à appliquer, est prévue.

3. Considérations générales

3.1. Notion

La notion de vidéosurveillance renvoie au fait de surveiller ou d'observer des biens ou personnes au moyen de caméras. Elle complète usuellement l'observation ou la surveillance menée par des personnes physiques. Plusieurs catégories de vidéosurveillance peuvent être distinguées selon le but et les modalités appliquées.

Selon le *but* de la mesure, l'on distingue la vidéosurveillance d'observation (surveillance d'un rayon déterminé accessible au public), la vidéosurveillance dissuasive (surveillance ouverte des lieux publics ou privés afin d'empêcher la commission d'infractions) et la vidéosurveillance invasive (surveillance secrète d'une personne particulière soupçonnée de s'adonner à une activité délictuelle)⁷. Prenant appui sur les *modalités*, l'on sépare la vidéosurveillance avec enregistrement (ou « informatisée »), dont les images et données sont fixées sur un support (analogique ou numérique) en vue d'une consultation ultérieurement dans le temps, et celle qui intervient sans enregistrement (ou « simple »), qui permet exclusivement d'observer et d'identifier les personnes se trouvant sur les lieux surveillés⁸.

D'autres critères peuvent également servir d'éléments de distinction :

- *la durée* : le système peut être installé pour une longue période de temps (déterminée, voire indéterminée) ou uniquement temporairement, par exemple pendant un évènement particulier ;
- *le type d'installation* : la caméra peut être montée sur un support fixe ou mobile, statique ou pilotée à distance, par exemple en étant fixée sur un drone ou un véhicule déterminé ;
- *le système de prise d'images* : le dispositif optique technique utilisé peut prendre diverses formes, par exemple une caméra ou un appareil photo à prises de vues à intervalles réguliers ;
- *les modalités de visionnage et d'accès* : les images récoltées par la vidéosurveillance peuvent être enregistrées et/ou visionnées en direct, mises à la disposition d'un cercle

⁷ Pour cette distinction en trois catégories, cf. notamment ALEXANDRE FLÜCKIGER/ANDREAS AUER, La vidéosurveillance dans l'œil de la Constitution, AJP/PJA 2006 924, p. 924. Voir également le Rapport du DFJP, Vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics, septembre 2007 (« Rapport DFJP »), p. 9.

⁸ FLÜCKIGER/AUER, *op. cit.*, p. 925.

déterminé de personnes et/ou plus largement accessibles, notamment par leur diffusion sur une plateforme déterminée (Internet, page web, intranet, etc.) ;

- *l'application de filtres* : le système de vidéosurveillance peut être doté de filtres permettant de brouiller automatiquement les objets et/ou personnes filmées avant l'enregistrement des images – selon le système appliqué, il peut être ou non possible d'utiliser une clé de déchiffrement afin de décoder les zones brouillées⁹.

3.2. Buts et intérêts en cause

Sous un angle sécuritaire, un système de vidéosurveillance pourra notamment être installé afin :

- d'accroître le sentiment de sécurité ou la sécurité elle-même ;
- de lutter contre la commission d'infractions ou les atteintes portées contre des personnes ou des biens, en les dissuadant (en cas de système visible) et/ou en facilitant l'établissement des faits ;
- lorsqu'il permet le visionnage des images en direct :
 - o de permettre une intervention rapide en cas d'infraction ou de soupçon d'acte répréhensible ;
 - o d'accroître l'efficacité des forces de police ou de surveillance sans trop augmenter leur effectif.

En parallèle toutefois, il implique également une atteinte à plusieurs droits et libertés. En font partie notamment la liberté personnelle et individuelle en général (art. 4 al. 1 Cst. VS), la garantie de l'intégrité physique et psychique, la liberté de mouvement (art. 10 al. 2 de la Constitution fédérale de la Confédération suisse [« Cst. »]¹⁰), le droit au respect de la sphère privée (art. 13 al. 1 Cst. et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales [« CEDH »]¹¹), la liberté de réunion et de manifestation (art. 8 et 10 Cst. VS ; art. 22 Cst.) et du droit d'être protégé contre l'emploi abusif des données personnelles (art. 13 al. 2 Cst.). Selon les modalités appliquées, la garantie de la propriété (art. 6 Cst. VS ; art. 26 Cst.) peut également être enfreinte¹². Une restriction à ces différents droits et libertés nécessite, selon le principe général de l'article 36 Cst., une base légale. Elle est d'ailleurs exigée par l'article 28 alinéa 1 lettre a LIPDA.

Spécifiquement sous l'angle de la protection des données, les images récoltées constituent des données à caractère personnel (art. 3 al. 3 LIPDA), en tout cas dans la mesure où elles

⁹ Rapport DFJP, p. 10.

¹⁰ RS 101.

¹¹ RS 0.101.

¹² Pour une vue d'ensemble de ces garanties et droits, FLÜCKIGER/AUER, *op. cit.*, p. 931 ss.

permettent l'identification des personnes filmées. La vidéosurveillance entraînera leur traitement (art. 3 al. 4 LIPDA), à la fois pour l'enregistrement des images, leur visionnage (avec ou sans l'enregistrement), leur utilisation, leur destruction ou encore leur transmission à un tiers. Soumis ainsi aux règles visant à assurer la protection des données, les systèmes de vidéosurveillance doivent en respecter les principes, dont principalement les principes de légalité (art. 17 al. 1 et 3 LIPDA), de proportionnalité (art. 17 al. 2 LIPDA), de finalité (art. 17 al. 2 LIPDA) et de sécurité (art. 21 LIPDA).

3.3. La situation réglementaire en Suisse

3.3.1. Sur le plan fédéral

Aucune base légale uniforme n'est actuellement prévue en matière de vidéosurveillance sur le plan fédéral. Contrairement à l'article 28 alinéa 1 lettre a LIPDA, la LPD n'impose en effet pas une base légale formelle dans tous les cas de vidéosurveillance.

La réglementation se caractérise plutôt par plusieurs fondements légaux différents, selon des domaines ou questions particulières. Peuvent par exemple être mentionnés :

- l'Ordonnance sur la vidéosurveillance dans les transports publics¹³, fondée notamment sur l'article 55 de la Loi sur le transport des voyageurs¹⁴ et l'article 16b de la Loi fédérale sur les chemins de fer¹⁵ ;
- l'article 15 de l'Ordonnance sur la sécurité relevant de la compétence fédérale¹⁶ ;
- l'article 108 de la Loi sur les douanes¹⁷ ;
- l'article 30 de l'Ordonnance sur les jeux de hasard et les maisons de jeu¹⁸ ;
- les articles 102 ss de la Loi fédérale sur les étrangers¹⁹, pour ce qui est spécifiquement de la récolte et de l'utilisation de données biométriques à des fins d'identification et de surveillance.

D'autres règles et dispositions peuvent impliquer la mise en place de systèmes de vidéosurveillance, sans que cela ne soit pour autant explicitement mentionné. Il s'agit par exemple des articles 122a ss de l'Ordonnance sur l'aviation²⁰ pour la sécurité dans les aéroports, ou de la Loi fédérale concernant la protection des ouvrages militaires²¹ ainsi que

¹³ RS 742.147.2.

¹⁴ RS 745.1.

¹⁵ RS 742.101.

¹⁶ RS 12.72.

¹⁷ RS 631.

¹⁸ RS 935.521.

¹⁹ RS 142.20.

²⁰ RS 748.01 ; pour sa référence dans ce contexte, et les règles de mises en œuvre, cf. le Rapport DFJP, pp. 16s.

²¹ RS 510.518.

l'Ordonnance concernant la protection des ouvrages militaires²² pour les installations exploitées ou utilisées par l'armée.

3.3.2. Sur le plan cantonal

Au niveau cantonal, la situation applicable en termes de réglementation liée à la vidéosurveillance est variée. A des fins d'illustrations, trois catégories de cantons peuvent être identifiées.

La première englobe tous les cantons qui ont adopté une loi spécifique sur la vidéosurveillance, soit :

- le canton de Fribourg (Loi du 7 décembre 2010 sur la vidéosurveillance et ordonnance du 23 août 2011 sur la vidéosurveillance²³) ;
- le canton de Zug (*Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum*²⁴ et *Verordnung zum Gesetz über die Videoüberwachung im öffentlichen und im öffentlich zugänglichen Raum*²⁵) ;
- le canton de Lucerne (*Gesetz über die Videoüberwachung*²⁶ et *Verordnung zum Gesetz über die Videoüberwachung*²⁷).

La seconde catégorie se compose des cantons qui, sans avoir une loi spéciale sur le sujet, disposent néanmoins de certaines règles traitant de la vidéosurveillance. Dans la plupart des cas, il s'agit de dispositions intégrées aux lois sur la protection des données et/ou aux réglementations légales de l'activité policière. L'on peut par exemple évoquer les cantons suivants :

- le canton de Vaud (art. 22 et 23 de la Loi sur la protection des données personnelles et art. 9 et 10 du Règlement d'application de la loi du 11 septembre 2007 sur la protection des données personnelles²⁸, ainsi que art. 21b de la Loi sur la police cantonale²⁹) ;

²² RS 510.518.1.

²³ RSF 17.3 et 17.31.

²⁴ BGS 159.1.

²⁵ BGS 159.11.

²⁶ SRL 39.

²⁷ SRL 39a.

²⁸ RSV 172.65 et 172.65.1.

²⁹ RSV 133.11.

- le canton de Genève (art. 42 de la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles³⁰ ainsi que art. 61 de la Loi sur la police³¹, à chaque fois mis en œuvre par les règlements de chacune des lois) ;
- les cantons de Neuchâtel et du Jura (art. 47 ss de la Convention intercantonale relative à la protection des données et à la transparence dans les cantons du Jura et de Neuchâtel³²) ;
- le canton de Berne (art. 51a ss de la Loi sur la police³³, mis en œuvre par l'Ordonnance sur la vidéosurveillance³⁴) ;
- le canton de Zurich (art. 32a ss *Polizeigesetz*³⁵ et *Verordnung über die Videoüberwachung im öffentlichen Verkehr*³⁶), qui intègre également un *Leitfaden* détaillant les modalités et règles générales applicables à la vidéosurveillance ;
- le demi-canton de Bâle-Ville (art. 17 et 18 de la *Gesetz über die Information und den Datenschutz*³⁷ et son ordonnance d'application) ;
- le demi-canton de Bâle-Campagne (art. 43 ss de la *Polizeigesetz*³⁸) ;
- le canton d'Uri (art. 33 de la *Polizeigesetz*³⁹, mis en œuvre par la *Videoverordnung*⁴⁰).

Enfin, une troisième catégorie regroupe tous les cantons qui ne disposent d'aucune réglementation particulière sur la vidéosurveillance. Tel est par exemple le cas du demi-canton d'Appenzell Rhodes-Intérieures ou des cantons des Grisons, de Soleure ou de Thurgovie (ce dernier disposant néanmoins d'un *Musterreglement* sur la question).

S'agissant des communes, plusieurs ont adopté une réglementation particulière en matière de vidéosurveillance, dont la ville de St Gall (*Reglement über die Videoüberwachung auf öffentlichem Grund*⁴¹ et *Reglement über die Videoüberwachung im Umfeld der Arena St.Gallen*⁴²) ou la ville de Genève (Règlement relatif à la vidéosurveillance en Ville de Genève⁴³). En Valais, l'on retrouve mention de la vidéosurveillance par exemple à l'article

³⁰ RS GE A 2 08.

³¹ RS GE F 1 05.

³² RSN 150.30.

³³ RS BE 551.1.

³⁴ RS BE 551.332.

³⁵ RS ZH 550.1.

³⁶ RS ZH 740.12.

³⁷ GS BS 153.260.

³⁸ GS BL 700.

³⁹ RB 3.8111.

⁴⁰ RB 3.8115.

⁴¹ sRS 412.4.

⁴² R 3293.

⁴³ LC 21 315.

21bis du Règlement communal de police de la Commune de Sion⁴⁴ ou dans le Règlement communal sur la vidéosurveillance de la Commune de Sierre. Ces textes reposent juridiquement sur les compétences réglementaires des communes et leur autonomie. Il est à noter que le sort de ces règlements suite à l'adoption du présent projet de loi y est traité à l'article 23 (dispositions transitoires).

4. Commentaire des dispositions

4.1. Article 1

Ce premier article exprime l'objet ainsi que le but de la loi.

L'alinéa 1 précise l'objet général de la loi. Il est complété par les articles 2 (définitions) et 3 (champ d'application). De façon générale, la loi a pour objet de fixer les conditions et modalités de la vidéosurveillance par une autorité dans les lieux publics. Trois éléments de rattachement peuvent être dégagés de cette formulation, soit (i) la vidéosurveillance (ii) dans un lieu public et (iii) l'existence d'une autorité. *A contrario*, la loi ne réglemente pas d'autres formes de traitement de données qui n'interviendrait pas par vidéosurveillance, ni cette dernière lorsqu'elle est mise en œuvre par des privés (et donc soumise à la LPD). La loi ne réglemente pas non plus la vidéosurveillance mise en place par une autorité ailleurs que dans un lieu public, notamment à l'intérieur d'immeubles faisant exclusivement partie de son patrimoine financier.

Ce champ d'application limité aux lieux publics s'explique pour deux motifs principaux. Premièrement, l'article 28 LIPDA lui-même se limite explicitement aux lieux publics. Deuxièmement, la vidéosurveillance dans des lieux publics porte une atteinte plus marquée aux droits du public que celle qui serait installée dans des lieux privés, en raison du nombre de personnes potentiellement concernées. Les conditions applicables et modalités ne peuvent donc pas être identiques.

Dans tous les cas, la vidéosurveillance qui ne porterait pas sur des lieux publics (et ne serait donc pas soumise à la LVID et LIPDA) serait régie par la LPD. Ce serait le cas plutôt théorique où l'État agirait comme un privé à l'intérieur d'un immeuble qui relève de son patrimoine financier.

L'alinéa 2 exprime le but de la loi qui doit permettre à une autorité d'installer des appareils de prises de vues et d'enregistrement d'images dans des lieux publics, mais également s'assurer que les systèmes de vidéosurveillance installés contribuent à la sécurité des personnes et des biens dans les lieux publics, à l'exclusion d'autres buts.

⁴⁴ R 5.1.

L'alinéa 3 enfin renvoie de façon générale aux dispositions de la LIPDA qui s'appliquent à titre supplétif. En particulier, les principes généraux de tout traitement de données (art. 17 ss LIPDA) et les limitations à la communication de telles données (art. 22 ss LIPDA), de même que les attributions du Préposé (art. 37 LIPDA), seront pleinement pertinents pour interpréter et appliquer la présente loi.

4.2. Article 2

Les définitions suivent la systématique de la LIPDA et visent à préciser les notions importantes utilisées.

L'alinéa 1 définit le terme central de vidéosurveillance. Le projet de loi vise exclusivement l'observation de personnes ou de biens au moyen de dispositifs techniques fonctionnant par l'image. Indépendante de la technologie utilisée, cette notion englobe par exemple les caméras vidéo, appareils photos à prises de vues régulières ou *webcams*, ainsi que toute autre technologie similaire qui n'existerait pas encore. La notion de vidéosurveillance est aussi indépendante du caractère temporaire ou définitif de l'installation de vidéosurveillance, de même que de l'éventuel support utilisé (drone, *dashcam*, etc.). La loi ne couvre en revanche pas les systèmes d'observation qui seraient basés sur d'autres caractéristiques que la prise d'images (enregistrement de sons, caméras thermiques, localisation de téléphones portables, etc.). Ces systèmes sont réservés à la police en application du CPP et/ou de l'article 42 LPol.

Bien que la loi vise à permettre la vidéosurveillance dans le but de contribuer à la sécurité des personnes et des biens (art. 1 al. 2), cela ne représente pas un élément de la définition de la vidéosurveillance. Sont ainsi également visées et couvertes par cette définition les installations de vidéosurveillance qui poursuivent un but purement récréatif ou d'observation générale. Elles ne seront toutefois admissibles qu'à la condition où elles ne permettent pas l'identification ou la reconnaissance de personnes (art. 3 al. 2 let. e).

L'alinéa 2 définit la notion de lieu public par deux caractéristiques : son rattachement au domaine public ou au patrimoine administratif (i), qu'il soit cantonal ou communal (à l'exclusion notamment des immeubles de la Confédération) (ii). Selon la jurisprudence fédérale, le patrimoine administratif comprend tous les biens des collectivités publiques qui sont directement affectés à la réalisation d'une tâche publique, dont les immeubles qui abritent les écoles, les hôpitaux, les gares, les musées, les bibliothèques et, de manière générale, les établissements publics et les services administratifs de l'État⁴⁵. Il se distingue du patrimoine financier, qui intègre les biens de l'État qui, n'étant pas affectés à une fin d'intérêt

⁴⁵ ATF 103 II 227, c. 3 ; arrêt du Tribunal fédéral 1C_379/2014 du 29 janvier 2015, c. 5.3.

public, ont la valeur d'un capital, peuvent produire un revenu (voire être réalisés) et sont en principe gérés selon le droit privé⁴⁶.

Cette définition ne dépend en revanche pas du caractère ouvert ou fermé du lieu public, ni de son accessibilité au public. Ce dernier point se justifie par le fait que l'État exploitant le domaine public ou le patrimoine administratif le fait dans le cadre de la réalisation d'une tâche publique. Il est alors intégralement soumis aux règles et principes de droit public, dont le principe de la base légale. L'installation d'un système de vidéosurveillance dans un immeuble relevant du patrimoine administratif requiert donc un fondement légal conformément aux articles 17 alinéa 1 LIPDA et 28 alinéa 1 lettre a LIPDA, ceci indépendamment du cercle des personnes qui peuvent y accéder. L'autorité peut avoir un intérêt à installer un système de vidéosurveillance dans un bâtiment relevant de son patrimoine administratif à la fois pour les pièces accessibles au public (salle d'accueil, guichets, etc.) et celles qui ne le sont pas, par exemple afin de s'assurer que des personnes non-autorisées n'y accèdent pas.

L'atteinte aux droits du public sera plus faible lorsque le système de vidéosurveillance est mis en place dans un lieu qui n'est pas librement accessible au public. Il s'agit toutefois là d'une caractéristique qui doit être considérée en lien avec l'autorisation et la pesée des intérêts (*cf.* art. 13 du projet de loi). D'autres lois pourront néanmoins entrer en considération pour décider des modalités du système dans certains cas particuliers, comme les règles de protection des travailleurs (spécialement l'art. 40 de la Loi sur le personnel de l'État du Valais⁴⁷ [LPersVS]) lorsqu'il est installé dans des locaux de travail.

L'alinéa 3 définit le terme d'autorité en renvoyant à la notion de l'article 3 alinéa 1 LIPDA pour assurer une homogénéité entre les deux lois.

L'alinéa 4 définit la vidéosurveillance avec diffusion, qui représente un cas particulier de vidéosurveillance dont les images (enregistrées ou non) sont diffusées et accessibles à un cercle de personnes déterminé ou indéterminé n'étant pas limité à l'autorité requérante, en particulier sur un site Internet ou Intranet, à l'image par exemple de *webcams* reprises sur une page Internet. Cela n'englobe en revanche pas les systèmes de vidéosurveillance dont la technologie de transmission des images se fonde sur l'utilisation d'une plateforme électronique *ad hoc* uniquement accessible aux personnes autorisées au sein de l'autorité requérante.

⁴⁶ Arrêt du Tribunal fédéral 1C_379/2014 du 29 janvier 2015, c. 5.3.

⁴⁷ RS VS 172.2.

L'alinéa 5 définit la vidéosurveillance temporaire, qui est soumise à un régime simplifié (art. 15). Il s'agit là également d'une forme particulière de vidéosurveillance, qui se distingue par sa durée de fonctionnement ou d'installation limitée. Elle vise notamment les cas de manifestations culturelles ou sportives.

4.3. Article 3

L'article 3 du projet définit le champ d'application de la loi.

Selon l'alinéa 1, la loi s'applique à toute vidéosurveillance mise en œuvre par une autorité dans un lieu public⁴⁸. La manière dont l'autorité procède pour cette mise en œuvre n'est pas pertinente dès le moment où elle exploite le système installé.

L'alinéa 2 opère une « précision négative » du champ d'application de la loi en excluant certains domaines ou cas déterminés. La liste est exhaustive.

Selon la lettre a, la loi ne s'applique pas à la vidéosurveillance ordonnée en application des dispositions du CPP ou de la LPol. Pour ce qui est d'abord du CPP, il s'agit essentiellement des mesures de surveillance secrètes des articles 269 ss CPP, dont la mise en œuvre de dispositifs techniques de surveillance conformément aux articles 280 ss CPP. Cette réserve s'impose au regard de la répartition des compétences entre cantons et Confédération, dans la mesure où le droit cantonal ne saurait déroger au droit fédéral (art. 49 Cst.). S'agissant ensuite de la réserve relative à la LPol, elle se justifie par le caractère spécial des règles qui y sont prévues. Les dispositions relatives à la vidéosurveillance correspondent en effet à certaines hypothèses particulières, qui imposent une compétence en faveur de la police cantonale. L'observation préventive (42 LPol), tout comme l'observation de l'article 282 CPP, est limitée aux cas dans lesquels existent des indices sérieux que des crimes et délits ont été ou peuvent être commis. Une contravention ne suffit pas. Toute surveillance dépassant un mois doit être autorisée par le ministère public et les personnes surveillées doivent être informées *a posteriori*. Il y a en outre un intérêt prépondérant à ne pas informer préalablement à la mise en place de la surveillance.

Quant à l'article 58 al. 2 LPol, il prévoit quatre types de surveillance. La lettre a permet la surveillance pour suivre directement ce qui se passe en un lieu déterminé et permettre à la police cantonale d'intervenir rapidement et de manière appropriée. Cette surveillance est limitée dans le temps et a pour seul but de guider les forces d'intervention. Si elle poursuit un autre but, notamment prévenir la commission d'un crime ou d'un délit, elle doit notamment répondre aux conditions de l'article 42 LPol. La lettre b vise la régulation du trafic, ce qui

⁴⁸ Cf. également les commentaires à l'article 1.

n'implique pas le traitement de données personnelles et, de ce fait, ne tombe pas dans le champ de la LIPDA ou de la LVid. Des mesures techniques doivent être prises pour que les personnes ne soient pas identifiables (y compris par exemple par l'enregistrement des plaques d'immatriculation des véhicules filmés) et les données ne devront jamais être utilisées dans un autre but. Si la surveillance est utilisée pour prévenir la commission d'infractions routières, c'est là encore les conditions de l'article 42 LPol qui trouveront application. La lettre c vise un cas particulier et très temporaire lié à des manifestations. Le risque de recoupement avec la LVid est tempéré par le caractère temporaire de la surveillance et limité aux actes (pénalement) punissables, ce qui justifie cette exception. C'est le lieu de préciser que la LPol vise principalement des installations temporaires et souvent mobiles, alors que la LVid vise de façon générale des installations durables (notamment vu la procédure simplifiée prévue pour la vidéosurveillance temporaire selon l'art. 15 LVid). Ainsi, et par exemple, la vidéosurveillance d'un cortège de supporters lors d'un événement sportif à risque entre la gare et le stade tombe dans le champ de l'article 58 alinéa 2 lettre c, voire de l'article 42 LPol. A l'inverse, l'installation de caméras permanentes autour du stade ou aux abords de la gare sera soumise et devra répondre aux conditions de la LVid, ceci même si ces systèmes ne sont exploités que lors des matchs.

Quant à l'article 58 alinéa 2 lettre d LPol, il s'agit d'une clause toute générale visant la prévention d'un crime ou d'un délit lorsque les autres modes d'intervention paraissent insuffisants, y compris la vidéosurveillance au sens de l'article 42 LPol. Les cas d'application de cette disposition apparaissent cependant peu évidents, dans la mesure où elle n'entre en principe en compte que si les conditions de l'article 42 LPol ne sont elles-mêmes pas remplies. Or, dans un tel cas, le recours à l'article 58 alinéa 2 lettre d LPol ne serait pas justifié et la jurisprudence du TF ne serait plus respectée. L'article 58 al. 2 lettre d LPol risque fort de ne jamais trouver application et cette disposition ne saurait donc faire obstacle à une application de la LVid dans le cas de systèmes de vidéosurveillance qui n'entreraient pas dans le champ d'application spécifique des articles 42, 58 al. 2 lettre a à c, et 59 LPol.

En résumé, lorsque ces dernières dispositions ne s'appliquent pas (y compris parce que les buts ou la durée de la vidéosurveillance en excluent l'application), les systèmes de vidéosurveillance sont soumis à la présente loi. Tel sera par exemple et notamment le cas des systèmes de vidéosurveillance installés au sein d'établissements de détention.

Selon les lettres b et c, la loi ne s'applique pas à la vidéosurveillance installée en application de l'Ordonnance sur la vidéosurveillance dans les transports publics⁴⁹ (OVid-TP) et dans d'autres domaines qui relèvent de la compétence fédérale. Il s'agit là encore de respecter la répartition des compétences entre cantons et Confédération et d'éviter d'enfreindre le principe de la primauté du droit fédéral de l'article 49 Cst. La lettre f rappelle également cela pour les systèmes de vidéosurveillance mis en place par des personnes privées sans lien avec une autorité, puisqu'ils sont soumis à la LPD.

La lettre d exclut du champ d'application de la loi un cas très particulier de vidéosurveillance sans possibilité d'enregistrement ni de diffusion, qui est exclusivement destinée et utilisée pour permettre l'entrée ou la sortie d'un immeuble, bâtiment ou installation appartenant ou exploité par des autorités, et dont le fonctionnement est déclenché par l'appel d'un utilisateur. Il s'agit là essentiellement du cas des interphones, qui n'affectent que de manière très limitée les droits des personnes concernées et dont le but ne correspond que très partiellement à ceux prévus par la loi. Il n'est pas nécessaire de les soumettre à autorisation, ni aux règles de contrôle strictes prévues par la loi. Ils seront en revanche intégralement soumis aux règles de la LIPDA, notamment pour ce qui est du devoir d'informer lors de la collecte (art. 19 LIPDA) et du principe de proportionnalité (art. 17 al. 2 LIPDA).

Selon la lettre e, la loi ne s'applique pas à la vidéosurveillance ne permettant aucune identification et aucune reconnaissance des personnes filmées. Cela englobe les systèmes de vidéosurveillance qui ne filment pas de personnes ou d'autres éléments liés à des personnes, ceux qui ne sont pas suffisamment précis pour permettre la reconnaissance des personnes filmées (à la condition qu'un traitement ultérieur des images ne le permette pas non plus), et ceux auxquels sont appliqués des filtres permettant de brouiller automatiquement les objets et/ou personnes filmées avant l'enregistrement des images, sans possibilité de décryptage (brouillage « en dur » ou irréversible). Cette exception s'explique par le fait que les droits à la protection des données des personnes entrant dans le champ optique du système de vidéosurveillance ne sont pas affectés dans de tels cas. D'autres droits, dont ceux à la protection de la personnalité, peuvent en revanche être concernés. Cela n'est toutefois pas suffisamment marqué pour imposer une application stricte de l'article 36 Cst. et la nécessité d'une base légale formelle.

Aucune réserve expresse n'est par contre faite en faveur des systèmes de caméras pouvant être mis en place par le garde-faune dans l'exercice de ses fonctions (notamment pour la surveillance et la gestion de la faune et du parc animal valaisan), en l'absence de base légale

⁴⁹ RS 742.147.2

existante. Ces systèmes ne visent pas à contribuer à la sécurité des personnes et des biens (but qui est couvert à la fois par l'article 28 LIPDA et l'article 1 al. 2 de la LVid). Ils présentent toutefois certains risques en termes de protection des données, notamment s'ils filment une zone habitée ou un lieu de passage fréquent. Une disposition *ad hoc* devrait dès lors être ajoutée dans la législation applicable, par exemple dans la Loi sur la chasse et la protection des mammifères et oiseaux sauvages (LcCh)⁵⁰. Elle pourrait renvoyer à la LVid. En l'absence d'une telle règle, le garde-faune devra installer un système de vidéo qui permet de flouter automatiquement les éventuelles personnes qui passeraient dans le champ optique des caméras.

L'alinéa 3 réserve le cas particulier dans lequel le système de vidéosurveillance installé par une personne privée et soumis à la LPD (art. 3 al. 2 let. f) conduit à un usage accru du domaine public. Tel sera pour l'essentiel le cas lorsque le système de vidéosurveillance filme le domaine public dans une mesure dépassant le simple usage « normal ». Les communes étant compétentes pour autoriser l'usage accru du domaine public, et d'arrêter les critères applicables, il leur appartient de régler ces cas lorsqu'un tel usage découle de systèmes de vidéosurveillance privés. Il ne s'agit pas ici prioritairement de protection des données, mais bien plus d'usage (accru) du domaine public pouvant être soumis à autorisation selon les règles générales, raison pour laquelle il est renvoyé au droit communal.

4.4. Article 4

L'article 4 du projet de loi décrit les principes généraux qui doivent régir tout système de vidéosurveillance mis en place par une autorité (identification des modalités, mise en place, exploitation, utilisation des données, etc.). Ils s'inspirent directement des principes généraux des art. 17 ss LIPDA.

L'alinéa 1, première phrase, reprend le but de l'article 1 alinéa 2 de la loi et y ajoute une exclusion de prise de son dans les modalités du système. Seul un système de vidéosurveillance ne permettant pas l'enregistrement du son peut donc être mis en place et exploité par une autorité conformément à l'article 28 LIPDA. Cette restriction s'impose dans la mesure où les droits des personnes concernées sont atteints plus fortement par un système qui cumulerait l'image et le son. Or, les buts poursuivis par le système de vidéosurveillance ne justifient pas une telle atteinte accrue. Des enregistrements sonores sans image ne sont pas non plus prévus par la loi.

⁵⁰ RS VS 922.1.

S'agissant de la deuxième phrase de l'article 4 alinéa 1, elle exprime le principe de finalité (art. 17 al. 2 LIPDA) qui exige que les données récoltées par le système de vidéosurveillance ne puissent être utilisées qu'au regard des buts fixés par l'autorisation, ceux-ci devant dans tous les cas respecter le cadre de l'article 28 LIPDA.

L'alinéa 2 reprend les principes de proportionnalité et de bonne foi (art. 17 al. 2 LIPDA). Le premier impose que la vidéosurveillance soit la moins intrusive possible au regard des buts poursuivis. Cela englobe les deux volets du principe que sont la règle de l'aptitude (le moyen choisi doit être apte à atteindre le but visé) et de la nécessité (le but ne peut être atteint par une mesure moins incisive). S'y ajoute la nécessité d'un rapport raisonnable entre le but et les intérêts publics ou privés compromis (principe de la proportionnalité au sens étroit).

L'alinéa 3 impose que la sécurité des données soit garantie (art. 21 LIPDA). Cette règle doit caractériser l'entier de l'exploitation du système de vidéosurveillance (identification des caractéristiques, mise en œuvre, sort des images récoltées, etc.). Le principe de la sécurité est particulièrement important dans le cadre d'un système de vidéosurveillance, vu les risques d'abus que cela comporte, par exemple en identifiant les habitudes d'une personne passant fréquemment dans un lieu donné ou en dévoilant des informations relevant de sa sphère intime. Toutes les mesures de sécurité suffisantes au regard des circonstances doivent donc être prises, dont (selon les cas) le cryptage des images. Des mesures techniques et organisationnelles doivent être prises pour s'assurer qu'un accès sans droit aux données soit exclu.

L'alinéa 4 affirme le principe de l'autorisation obligatoire du système de vidéosurveillance (art. 9 al. 1) ou, exceptionnellement, de la notification pour la vidéosurveillance temporaire (art. 15). A défaut d'une telle autorisation, le système sera qualifié d'illicite, avec toutes les conséquences que cela entraîne pour la validité et l'utilisation possible des données récoltées (moyen de preuve illicite). Cette même conséquence affectera le système de vidéosurveillance qui ne respecte pas les contours d'une autorisation.

L'alinéa 5 enfin affirme le respect de la propriété privée (garantie par les articles 26 Cst. et 6 Cst. VS). Tout système de vidéosurveillance qui devrait être placé sur une propriété privée ne le pourra qu'à la condition d'obtenir l'accord du propriétaire ou de procéder par la voie de l'expropriation, conformément à la Loi sur les expropriations⁵¹. Le champ optique du système de vidéosurveillance pourrait également, dans certains cas, porter atteinte à la propriété privée de personnes, par exemple s'il filme un immeuble ou un terrain appartenant à une personne privée.

⁵¹ RS VS 710.1.

4.5. Article 5

L'article 5 précise qui, au sein de l'autorité requérant et exploitant le système de vidéosurveillance, doit être considéré comme responsable du système (al. 1) et quelles compétences lui reviennent (al. 2).

Les différentes hypothèses abordées à l'alinéa 1 tiennent compte des formes que peuvent revêtir les autorités au sens de l'art. 3 al. 1 LIPDA (*cf.* la définition de l'art. 2 al. 3 de la loi). Dans tous ces cas, le responsable du système correspond à la personne ou organe qui occupe une fonction de décision au sein de l'autorité, lui permettant d'influencer directement la manière dont celle-ci exploite et utilise le système de vidéosurveillance en vue d'assurer le respect du projet de loi.

L'alinéa 2 détaille les compétences du responsable du système, qui sont formulées comme de véritables devoirs. Il est ainsi responsable :

- de notifier le projet de vidéosurveillance et/ou requérir la délivrance d'une autorisation auprès de l'autorité compétente (let. a) : cela implique notamment qu'il vérifie que les différentes conditions de la demande d'autorisation sont remplies, que le système de vidéosurveillance projeté respecte les conditions de la loi et qu'il signe la demande d'autorisation. Ce dernier point formel vise à assurer que les autres devoirs de vérification ont été respectés par le responsable du système.
- d'obtenir si nécessaire l'accord du propriétaire d'un immeuble, un bien ou une parcelle privé sur lequel le système de vidéosurveillance doit être mis en place (let. b) : il s'agit là d'un renvoi au principe de l'article 4 alinéa 5. Si l'accord ne peut pas être obtenu, il lui revient d'initier la procédure d'expropriation.
- d'exploiter le système de vidéosurveillance et s'assurer du respect des conditions et modalités posées dans la présente loi et l'autorisation (let. c) : les devoirs du responsable du système d'assurer le respect de la loi s'étendent à toute la durée d'exploitation du système. S'il délègue cette tâche, le responsable du système doit mettre en place les conditions et modalités nécessaires pour assurer le respect des conditions et modalités de l'autorisation (choix du délégataire, instructions et surveillance).
- de répondre aux requêtes émises par des personnes privées en lien avec le système de vidéosurveillance (let. d) : le système de vidéosurveillance menant à la récolte et au traitement de données personnelles, les personnes concernées disposent d'un droit d'obtenir des renseignements et de consulter leurs données (art. 31 et 32 LIPDA). Le

responsable du système a la compétence de répondre aux requêtes, y compris d'apprécier les éventuelles restrictions qui peuvent y être portées.

4.6. Article 6

L'article 6 pose un principe général relatif à la vidéosurveillance avec diffusion (définie à l'art. 2 al. 4), dont cette dernière caractéristique atteint fortement les droits des personnes filmées. Elle n'est pas prévue par l'article 28 LIPDA et la diffusion des images paraît difficilement apte à atteindre le but d'observation ou de dissuasion visé par cette norme.

Elle vise plutôt à offrir au public la possibilité de visionner des images d'un lieu particulier, le plus souvent en direct (*webcams*). Les intérêts de communication et de publicité ne sauraient contrebalancer une atteinte sérieuse aux droits fondamentaux des personnes filmées. Partant, ce type de vidéosurveillance doit être limité aux cas dans lesquels des personnes ne sont pas reconnaissables. Ce raisonnement doit être étendu à toute donnée personnelle récoltée par le système de vidéosurveillance, comme les plaques d'immatriculation des véhicules.

Un système de vidéosurveillance avec diffusion ne permettant pas la reconnaissance des personnes et autres données personnelles filmées intégrerait l'exception de l'article 3 alinéa 2 lettre d de la loi. L'article 6 rappelle ainsi cette exception. S'il permet en revanche la reconnaissance des personnes filmées ou de données personnelles (dont des plaques minéralogiques), un système de vidéosurveillance ne saurait faire l'objet d'une diffusion, à moins que celle-ci soit uniquement destinée aux personnes autorisées à visionner et faire usage des images récoltées au sein de l'autorité requérante.

4.7. Article 7

L'alinéa 1 introduit la notion de règlement d'utilisation. Celui-ci se retrouve dans d'autres dispositions de la loi, notamment à l'article 11 alinéa 3 qui requiert qu'il accompagne toute demande d'autorisation et soit remis à l'autorité compétente. Il doit permettre à l'autorité compétente de comprendre au mieux le système envisagé et de s'assurer qu'il respecte les principes et exigences de la loi, notamment de l'article 4. Il doit aussi permettre à l'autorité requérante d'assurer une exploitation conforme dans la durée.

Sous l'angle de son contenu, l'alinéa 2 requiert qu'il décrive au-moins l'installation de vidéosurveillance (y compris ses aspects techniques), définisse les personnes qui sont autorisées à visionner les images récoltées et détailler les mesures qui sont prises afin de répondre aux exigences et principes de la loi, notamment de l'article 4 et plus spécialement encore en termes de sécurité. L'autorité requérante est libre d'y ajouter d'autres éléments

pertinents, dans la mesure où ils se rapportent directement au fonctionnement et à l'utilisation du système de vidéosurveillance. Toute éventuelle technique complémentaire qui s'ajouterait à l'enregistrement des images (système de zoom, reconnaissance automatique des visages, suivi de personnes, fonctionnement en commun avec d'autres caméras, contrôle de badges, etc.) doit également être mentionnée dans le règlement d'utilisation.

L'alinéa 3 impose que le règlement d'utilisation soit tenu à jour par le responsable du système, notamment pour tenir compte des évolutions techniques.

4.8. Article 8

L'article 8 traite explicitement de la durée de conservation des images qui peuvent être enregistrées par le système de vidéosurveillance, selon les modalités autorisées.

L'alinéa 1 met en œuvre les principes de proportionnalité et de finalité, en exigeant que les données enregistrées soient détruites aussitôt qu'elles ne sont plus utiles au regard des buts poursuivis. Dans tous les cas, la conservation des images ne peut excéder la durée maximale de conservation qui est indiquée dans l'autorisation (art. 13 al. 4 let. c de la loi). Cette durée doit être fixée par l'autorité compétente au regard de l'entier des circonstances et modalités prévues pour le système de vidéosurveillance.

La loi précise explicitement que la durée de conservation sera en principe de 96 heures, sauf circonstances particulières. Cette réserve vise notamment les systèmes mis en place dans un lieu faisant souvent l'objet d'infractions qui ne sont pas identifiables rapidement. Indépendamment de la marge de manœuvre de l'autorité compétente, elle ne peut prévoir une durée supérieure à 100 jours, en ligne avec la jurisprudence du Tribunal fédéral⁵².

L'alinéa 2 exprime une conséquence de la durée maximale de conservation, qui doit valoir pour les images enregistrées elles-mêmes ainsi que toute copie ou autre reproduction qui en aurait été faite. Des copies peuvent néanmoins être conservées au-delà de la durée maximale exprimée à l'article 8 alinéa 1 lorsque toute reconnaissance des personnes filmées est rendue définitivement impossible par des mesures techniques.

L'alinéa 3 réserve l'éventualité d'une production et d'une utilisation des images et données enregistrées dans une procédure judiciaire (civile, pénale ou administrative). Ces procédures judiciaires répondent à des règles et modalités qui leur sont propres, y compris pour le traitement de données.

4.9. Article 9

L'article 9 reprend le principe général de l'autorisation mentionné à l'article 4 alinéa 4.

⁵² ATF 136 I 87, c. 8.4 ; ATF 133 I 77, c. 5.

L'alinéa 1 pose ce principe, tout en réservant le cas de la vidéosurveillance temporaire qui n'est soumise qu'à notification du Préposé (art. 2 al. 5 et 15 de la loi). En-dehors de cette dernière hypothèse, le principe de l'autorisation s'applique quelles que soient les modalités choisies pour le système, dont l'enregistrement ou non des images.

L'alinéa 2 met en œuvre cette règle et précise la sanction. Toute mise en place d'un système de vidéosurveillance avant l'octroi de l'autorisation est illicite. Aucune exception à cette règle n'est prévue et l'autorité compétente ne peut pas autoriser provisoirement un système de vidéosurveillance avant analyse des conditions. L'autorité requérante ne peut pas non plus exploiter un système de vidéosurveillance pendant la procédure d'autorisation, sous réserve du délai transitoire d'une année suivant l'entrée en vigueur de la loi (art. 22 al. 1). Cette application stricte du principe de l'autorisation s'impose compte tenu des atteintes aux droits de l'administré que ce type de système peut impliquer.

4.10. Article 10

L'article 10 confère une compétence de préavis au Préposé. Bien qu'il ne soit pas l'autorité compétente pour octroyer l'autorisation (*cf.* art. 12 de la loi), le Préposé joue un rôle central en termes de protection des données au niveau cantonal. La mission et les compétences qui lui sont confiées par la LIPDA (art. 37 LIPDA) imposent de lui soumettre le projet de vidéosurveillance pour préavis. C'est bien le Préposé qui est compétent, et non la CCPDT (art. 38 et 39 LIPDA), dans la mesure où celle-ci dispose plutôt d'attributions de surveillance générale dans le domaine de la protection des données.

L'alinéa 1 impose à l'autorité requérante de soumettre son projet de vidéosurveillance au Préposé. Afin d'assurer une information complète du Préposé, cette disposition précise les informations qui doivent lui être communiquées par renvoi au contenu minimum de la demande d'autorisation selon l'article 11 alinéa 2 de la loi. Dans les faits, l'autorité requérante pourra transmettre son projet de demande d'autorisation directement au Préposé. Ce dernier pourra requérir tout complément d'information nécessaire.

L'alinéa 2 octroie au Préposé un délai d'un mois pour formuler un éventuel préavis sur le projet de vidéosurveillance. Il s'agit là d'une *faculté* du Préposé et non d'une obligation. Dans le choix de se prononcer ou non sur un projet, le Préposé devra notamment tenir compte de (i) son étendue, (ii) ses conséquences sur les droits fondamentaux, (iii) le lieu visé par la vidéosurveillance et (iv) les méthodes mises en œuvre. Par principe, le Préposé devrait rendre un préavis lorsqu'un système de vidéosurveillance soulève des questions particulières ou s'avère particulièrement délicat. L'absence d'un préavis explicite équivaut à une réponse positive. L'éventuel préavis devra être communiqué directement à l'autorité requérante.

A la suite de ce dernier point, l'alinéa 3 offre la possibilité au Préposé de prolonger le délai de préavis à un maximum de trois mois. Une telle prolongation n'est pas automatique, mais doit répondre à trois conditions essentielles. Il est ainsi nécessaire (i) qu'elle soit notifiée à l'autorité requérante, (ii) avant l'échéance du délai d'un mois de l'article 10 alinéa 2 et (iii) qu'elle soit justifiée par l'existence de circonstances particulières, dont la complexité du projet ou un grand nombre de demandes déposées simultanément. Le Préposé devra indiquer le motif invoqué dans sa notification de prolongation. La prolongation doit rester exceptionnelle mais sera certainement nécessaire avec l'entrée en vigueur de la loi et un nombre de demandes importantes déposées simultanément.

4.11. Article 11

L'article 11 détaille le contenu de la demande d'autorisation qui doit être présentée et signée par le responsable du système (art. 5 al. 2 let. a du projet de loi).

L'alinéa 1 requiert du Préposé qu'il publie un modèle de demande d'autorisation, ce qu'il pourra faire sur son site web. Cette règle a pour but d'assurer l'homogénéité des demandes et surtout de faciliter le travail des autorités. L'autorité requérante n'a toutefois pas l'obligation d'utiliser le modèle de demande d'autorisation.

L'alinéa 2 détaille le contenu de la demande d'autorisation par une liste non-exhaustive. Ce dernier point permet de tenir compte de la variété des situations envisageables et autorise l'autorité requérante à préciser d'éventuelles caractéristiques supplémentaires souhaitées. Les informations minimales requises sont les suivantes :

- le responsable du système (let. a) : la demande d'autorisation doit mentionner le nom et la fonction du responsable du système (art. 5 de la loi).
- la description du système de surveillance projeté (let. b) : le système de surveillance doit faire l'objet d'une description générale, au regard de ses caractéristiques et modalités.
- la zone à surveiller et l'emplacement des caméras (let. c) : la demande d'autorisation doit décrire avec suffisamment de précision la zone qui sera surveillée par le système de vidéosurveillance ainsi que l'emplacement des caméras. L'autorité requérante pourra joindre un plan pour faciliter la lecture de la demande.
- la raison et le but de la vidéosurveillance (let. d) : en vue du respect des principes de proportionnalité et de finalité, la demande d'autorisation doit préciser la raison et le but de la vidéosurveillance (objectifs généraux poursuivis, avantages, motifs ayant

justifié la mise en place, etc.). Ces éléments doivent s'inspirer de la description générale mentionnée à la lettre b.

- les personnes ayant le droit d'accéder aux enregistrements (let. e) : le cercle exact des personnes ayant le droit d'accéder aux enregistrements, identifiées par leur fonction au sein de l'autorité requérante, devra être décrit. Il s'agira de tenir compte dans ce cadre du principe de proportionnalité et de limiter le plus possible les personnes ayant accès aux enregistrements, selon les buts et les objectifs poursuivis.
- les mesures de sécurité prévues (let. f) : vu leur importance (art. 4 al. 3 de la loi), ces mesures doivent être décrites suffisamment précisément dans la demande d'autorisation, y compris pour ce qui relève de leur volet technique. Les informations liées à la sécurité ne seront évidemment pas rendues publiques.
- l'horaire de fonctionnement prévu (let. g) : conformément au principe de proportionnalité, le système de vidéosurveillance ne doit fonctionner que durant les heures absolument nécessaires à la poursuite des buts. A titre d'exemple, un système de vidéosurveillance placé aux abords d'un stade de football en vue de prévenir et poursuivre d'éventuelles infractions commises les soirs de match ne devrait fonctionner qu'à ces moments.
- la durée de conservation maximale des données enregistrées souhaitée (let. h) : dans le cas d'un système intégrant l'enregistrement des images, la demande d'autorisation doit préciser la durée maximale de conservation des données ainsi enregistrées, au regard du principe de l'article 8 alinéa 1 de la loi – à défaut d'une précision explicite, la durée requise sera considérée comme étant de 96 heures.
- l'analyse des risques et des mesures de prévention possibles, de même qu'une description du caractère proportionné du système (let. i) : la demande d'autorisation doit comporter une analyse des risques et mesures de prévention possibles. Il s'agit notamment d'identifier les risques du système pour les droits fondamentaux des personnes filmées, en général et en cas de faille de sécurité. Le sort de la pesée des intérêts entre ces risques et les avantages du système pour l'autorité, de même que les mesures prises pour répondre à ces risques, doivent également être décrits. Enfin, l'analyse doit souligner le caractère proportionné du système, en indiquant (i) pourquoi un système moins intrusif ne suffirait pas à atteindre les buts poursuivis et (ii) en quoi le système prévu répond aux exigences de proportionnalité.

- le préavis du Préposé ou à défaut la preuve de sa consultation (let. j) : dans la mesure où le Préposé a rendu un préavis, la demande d'autorisation doit l'intégrer. Si le préavis est négatif, l'autorité requérante pourra adapter sa demande pour tenir compte des recommandations du Préposé. En l'absence d'un préavis, l'autorité requérante devra joindre le courrier adressé au Préposé, par lequel elle lui soumet le projet pour préavis.

Selon l'alinéa 3, la demande d'autorisation doit être complétée par le règlement d'utilisation (art. 7 de la loi).

4.12. Article 12

L'article 12 identifie l'autorité compétente pour l'octroi de l'autorisation.

Une distinction fondamentale est opérée à l'alinéa 1 entre le niveau cantonal et communal. Afin de respecter le principe d'autonomie communale (art. 50 al. 1 Cst. et art. 70 Cst. VS), le Conseil d'État n'a pas été retenu comme autorité unique. Le projet prévoit ainsi deux autorités compétentes différentes, selon que l'autorité requérante est cantonale ou communale :

- si l'autorité requérante est cantonale, l'autorité compétente sera le Conseil d'État ;
- si l'autorité requérante est communale, l'autorité compétente sera le Conseil communal.

Dans les deux cas, l'autorité compétente est donc l'autorité exécutive du niveau considéré.

L'alinéa 2 exclut toute transmission de la compétence du Conseil d'État, qui ne saurait donc déléguer son pouvoir de décision lié à une demande d'autorisation présentée par une autorité requérante cantonale. Il est en effet essentiel que le Conseil d'État lui-même soit au courant du nombre de demandes déposées et du nombre d'autorisations octroyées, vu l'importance de l'atteinte aux droits fondamentaux des personnes concernées par les systèmes de vidéosurveillance.

Nonobstant cette dernière remarque, il n'est pas exclu pour le Conseil communal de pouvoir transmettre sa compétence de décision au Conseil d'État, comme cela est prévu à l'alinéa 3. Cette éventualité vise principalement le cas des communes de petite taille qui ne disposent pas d'une infrastructure suffisante pour examiner correctement l'entier des éléments impliqués dans la demande d'autorisation. Ces communes doivent dès lors pouvoir déléguer leur pouvoir de décision au Conseil d'État qui, fort de sa pratique au niveau cantonal ainsi que de la vue d'ensemble dont il dispose à ce titre, pourra être plus à même de traiter efficacement les demandes d'autorisation. Cette délégation peut intervenir en tout temps et est révocable,

mais doit être générale (et non limitée à un cas particulier). Elle doit prendre la forme d'une décision du Conseil communal notifiée formellement au Conseil d'État.

Lorsque le Conseil communal décide de déléguer sa compétence au Conseil d'État, ce dernier a l'obligation de l'accepter. Dans la mesure où la décision de délégation provient du Conseil communal lui-même, elle ne constitue pas une atteinte au principe de l'autonomie communale.

4.13. Article 13

L'article 13 précise les conditions auxquelles l'autorisation peut être octroyée par l'autorité compétente, sa durée, son éventuel renouvellement ainsi que son contenu minimum.

L'alinéa 1 pose deux conditions qui doivent nécessairement être réalisées pour que l'autorisation puisse être accordée :

- l'autorité requérante doit avoir déposé une demande d'autorisation remplissant les critères et conditions de la loi (let. a) ;
- les mesures énoncées dans le règlement d'utilisation doivent paraître suffisantes pour assurer le respect de la loi et de la LIPDA (let. b), dont les principes de l'article 4 de la loi.

L'alinéa 2 précise la durée maximale de l'autorisation, qui doit être limitée à ce qui est absolument nécessaire au regard des buts poursuivis. A titre d'exemple, si un système de vidéosurveillance a pour but de surveiller un chantier lié à un lieu public, l'autorisation devra correspondre à la durée du chantier. Si la vidéosurveillance est envisagée de manière permanente, l'autorisation ne peut être donnée pour une durée supérieure à cinq ans et, à moins d'un renouvellement (selon l'al. 3), prend automatiquement fin. Le système de vidéosurveillance devra alors être mis hors-service et démonté. C'est le meilleur moyen d'assurer un contrôle régulier des autorisations et de la conformité des installations.

Selon l'alinéa 3, l'autorisation est renouvelable, à chaque fois aux mêmes conditions et limites (notamment en ce qui concerne la durée de l'autorisation selon l'al. 2 précédent). Le nombre de renouvellements est théoriquement illimité, dans la mesure où cela respecte toujours les principes de la loi ainsi que de la LIPDA, dont ceux de proportionnalité et de finalité. Afin de permettre à l'autorité compétente d'évaluer correctement la possibilité d'un renouvellement, la demande de renouvellement doit reprendre l'entier des informations prévues à l'article 11 alinéa 2 et y ajouter une description de l'efficacité du système de vidéosurveillance au regard des buts poursuivis. Cette description doit détailler les effets positifs de la vidéosurveillance

tel qu'appliquée, les problèmes rencontrés, les solutions apportées ainsi que les motifs pour lesquelles le renouvellement de l'autorisation est nécessaire.

Le détail de l'autorisation est donné à l'alinéa 4, qui fait une liste non-exhaustive des éléments devant y figurer. Il s'agit :

- de plusieurs éléments figurant dans la demande d'autorisation selon l'article 11 alinéa 2 lettre a à h (let. a), cas échéant adaptés aux modifications, ajouts et changements imposés par l'autorité compétente. La description générale du système doit, dans l'ensemble, être le plus précis possible afin de le cadrer aux buts et objectifs poursuivis ;
- la nécessité d'indiquer l'existence du système de vidéosurveillance et la manière de le faire (let. b) : il s'agit là d'un renvoi aux règles de signalisation de l'article 20 de la loi, qui peut intégrer une reproduction imagée des panneaux et indications devant figurer sur les lieux ;
- la durée de conservation maximale des données enregistrées (let. c) : cette précision fait écho à l'article 8 de la loi ;
- cas échéant, d'éventuelles conditions supplémentaires (let. d) : l'autorité compétente demeure libre de fixer des conditions supplémentaires au système de vidéosurveillance, dans la mesure où ces conditions sont nécessaires pour assurer le respect des principes de la loi et/ou de la LIPDA ou de toute autre réglementation qui s'imposerait à l'autorité. L'autorité devra déterminer quels effets donner à ces conditions, notamment si elles sont suspensives ou résolutives.
- les voies de droit contre la décision (let. e) : la décision doit préciser les voies de droit qui existent à son encontre, au regard de l'article 14 alinéa 3 à 5 de la loi.

En plus des informations ainsi requises, l'alinéa 5 exige que la décision explique les motifs pour lesquels le préavis du Préposé n'aurait pas (totalement ou en partie) été suivi, lorsque tel est le cas. Cette indication doit être suffisamment détaillée pour permettre de comprendre les motifs de ce choix, à la fois en fait, en droit et sur les aspects techniques. L'explication ainsi donnée doit permettre cas échéant au Préposé de former recours contre l'autorisation, conformément à l'article 14 alinéa 3 de la loi.

4.14. Article 14

L'article 14 traite de la notification et publication de l'autorisation, ainsi que des voies de droit.

L'alinéa 1 précise comme suit les personnes auxquelles la décision doit être notifiée, selon les voies ordinaires utilisées pour la notification de décisions administratives :

- l'autorité requérante ; ainsi que
- le Préposé, afin qu'il puisse valablement contrôler que le système de vidéosurveillance autorisé respecte en tous points les dispositions de la LIPDA et puisse, selon les cas, s'y opposer conformément à l'alinéa 3.

L'alinéa 2 impose, en plus de la notification, que l'autorisation soit publiée dans le Bulletin officiel du canton du Valais. Cette exigence vise d'une part à permettre au public d'être tenu au courant des différentes autorisations qui sont délivrées et, d'autre part, à offrir une possibilité de contestation aux personnes qui seraient spécialement touchées par le système de vidéosurveillance. Une notification personnelle à chacune de ces personnes n'est en revanche pas envisageable, dans la mesure où tant l'autorité requérante que l'autorité compétente n'en connaîtront généralement pas le cercle avec précision. En exception à ce constat, une notification personnelle doit se faire, cas échéant, à la personne privée sur la propriété de laquelle sera installé tout ou une partie du système (*cf.* art. 4 al. 5 de la loi). Cela a pour but d'offrir à la personne privée une information directe du fait que le système affectera sa propriété privée.

Il n'est en revanche pas nécessaire de publier l'intégralité de l'autorisation. La publication des mesures de sécurité serait par exemple contre-productive. La loi se contente donc d'un extrait qui doit permettre à toute personne concernée de savoir où, quand, par qui et dans quel but elle est filmée.

L'alinéa 3 traite des voies de droit qui existent à l'encontre de la décision. Compte tenu de la marge de manœuvre qui est laissée à l'autorité compétente, il s'impose d'organiser les voies de droit en deux temps. La personne ou l'entité souhaitant contester la décision, d'octroi ou de refus de l'autorisation, devra en premier lieu former réclamation auprès de l'autorité compétente. Cette dernière pourra sur cette base revoir sa décision et, cas échéant, en rendre une nouvelle à la lumière des arguments avancés dans le contexte de la réclamation (*cf.* art. 34a ss de la Loi sur la procédure et la juridiction administratives⁵³ [LPJA]).

Le cercle des personnes pouvant former réclamation intègre l'autorité requérante, le Préposé ainsi que toute personne spécialement touchée par le système de vidéosurveillance. Cette dernière référence est un renvoi à la qualité pour recourir selon l'article 44 alinéa 1 lettre a LPJA (applicable à la procédure de réclamation par renvoi de l'art. 34b LPJA).

⁵³ RS VS 172.6.

L'alinéa 4 rappelle le principe de l'article 34e alinéa 3 LPJA, selon lequel seule la décision sur réclamation est sujette à recours. Ainsi, tout recours qui serait formé selon les articles 41 ss LPJA devra porter sur la décision sur réclamation et non sur l'autorisation elle-même. Le droit de recours appartient au même cercle de personnes que celles qui peuvent former réclamation selon l'al. 3, lui-même identifié selon l'article 44 LPJA.

L'alinéa 5 confirme l'application des règles de la LPJA à toute procédure de réclamation et de recours fondée sur le projet de loi.

4.15. Article 15

L'article 15 vise à instaurer une procédure simplifiée applicable à la vidéosurveillance temporaire au sens de l'article 2 alinéa 5 de la loi. Considérant la définition stricte de vidéosurveillance temporaire, ces installations présentent un plus faible risque d'atteinte aux droits fondamentaux. La procédure d'autorisation classique apparaît comme disproportionnée avec la durée d'engagement de la vidéosurveillance.

L'alinéa 1 pose la règle générale selon laquelle les systèmes de vidéosurveillance temporaires ne sont pas soumis à autorisation. Il s'agit là d'une dérogation au principe général de l'autorisation de l'article 9 de la loi.

L'alinéa 2 maintient l'application pleine et entière des principes de la loi (notamment de l'art. 4) ainsi que de la LIPDA également à l'égard de tels systèmes de vidéosurveillance temporaire. Le système de vidéosurveillance temporaire devra notamment tenir compte et respecter pleinement les principes de proportionnalité, finalité et de bonne foi.

L'alinéa 3 pose une obligation d'information à charge du responsable du système en faveur du Préposé, au moins deux mois avant la mise en œuvre. Cette obligation remplace la demande d'autorisation et vise à assurer un certain contrôle de ce type d'installation. Elle est posée en faveur du Préposé, dans la mesure où le contrôle général de la LIPDA lui revient. En l'absence d'une autorisation de la part de l'autorité compétente, celle-ci n'a pas à être informée.

L'alinéa 4 requiert que l'information précise plusieurs des points exigés dans le cadre de la demande d'autorisation, soit :

- le responsable du système ;
- la zone à surveiller et l'emplacement des caméras ;
- la raison et le but de la vidéosurveillance ;
- les personnes ayant le droit d'accéder aux enregistrements ;
- les mesures de sécurité prévues ;

- la description du système de surveillance projeté ;
- l'horaire de fonctionnement prévu ;
- la durée de conservation maximale des données enregistrées souhaitée pour les systèmes intégrant l'enregistrement ;
- l'analyse des risques et des mesures de prévention possibles au regard du but poursuivi, de même qu'une description du caractère proportionné du système.

Ces informations sont nécessaires au Préposé pour qu'il puisse correctement identifier les éventuels problèmes et atteintes qui découlent du système de vidéosurveillance temporaire. Elles sont donc nécessaires également dans le contexte de la procédure simplifiée. Le Préposé devra toutefois tenir compte du caractère simplifié de la procédure et ne pas poser d'exigences trop strictes quant au détail et à la précision des informations données conformément à l'alinéa 4. Il suffit que les informations soient complètes et permettent d'apprécier le système projeté. Il en va de même pour le règlement d'utilisation prévu par l'article 7 de la loi, mais dont on admettra qu'il soit sommaire.

L'alinéa 5 confère au Préposé la compétence de proposer des adaptations et conditions au système envisagé, dans le but d'assurer le respect de la présente loi et des principes plus généraux de la LIPDA.

Lorsque de telles conditions et adaptations sont requises par le Préposé, l'alinéa 6 en précise les effets. Dénuées d'effets contraignants formels *avant* la mise en œuvre du système, leur refus par le responsable du système obligera l'autorité requérante à suivre la procédure ordinaire d'autorisation des articles 9 ss. Autrement dit, le fait de refuser les conditions et adaptations proposées par le Préposé mène à une procédure plus longue et complète. Dans un tel cas, la proposition du Préposé vaudra préavis au sens de l'article 11 alinéa 2 lettre j du projet de loi. Vu les conséquences importantes du préavis, le Préposé s'efforcera, sauf atteinte importante aux droits des personnes concernées, de recommander des adaptations facilement réalisables dans le bref délai à disposition.

4.16. Article 16

L'article 16 affirme le principe d'une évaluation annuelle du système.

Conformément à l'alinéa 1, il appartient au responsable du système d'évaluer au moins une fois par année la nécessité et l'efficacité du système de vidéosurveillance. Cela doit intervenir au regard des buts poursuivis et de l'autorisation qui a été accordée conformément à l'article 13 de la loi. Il s'agit essentiellement pour le responsable du projet de s'assurer que le système

respecte bien les limites de la loi et l'autorisation, dont les principes de proportionnalité et de finalité.

L'alinéa 2 impose au responsable du système de consigner par écrit la réalisation de cette évaluation annuelle ainsi que ses résultats. Le rapport ainsi établi doit (i) décrire l'évaluation effectuée, (ii) consigner ses résultats et (iii) les apprécier précisément au regard des exigences légales et des modalités de l'autorisation. Ce rapport n'a pas à être transmis automatiquement à l'autorité compétente ou au Préposé, mais doit être tenu à leur disposition s'ils souhaitent le consulter. Considérant cette règle, le rapport doit être rédigé d'une façon suffisamment claire et précise pour permettre à l'autorité compétente ou au Préposé de le comprendre dans son entier. Il peut être succinct, le but principal du rapport étant de s'assurer que le responsable du système a procédé à l'évaluation.

4.17. Article 17

L'article 17 identifie les compétences de contrôle de l'autorité compétente et du Préposé.

Selon l'alinéa 1, la compétence principale en la matière revient à l'autorité compétente ayant délivré l'autorisation, qui peut en tout temps procéder à des contrôles du système. Elle peut en particulier se rendre sur place et demander à consulter le rapport d'évaluation annuelle de l'article 16. Cette compétence est en particulier justifiée par le droit de l'autorité compétente de révoquer l'autorisation (art. 18).

L'alinéa 2 ajoute une compétence de vérification et de contrôle en faveur du Préposé. Il s'agit là des mêmes pouvoirs de vérification que ceux revenant à l'autorité compétente selon l'alinéa 1, notamment pour ce qui est de la possibilité de se rendre sur place et de demander à consulter le rapport d'évaluation annuelle. Le but du contrôle du Préposé consiste plus largement à s'assurer que le système de vidéosurveillance respecte les principes de la loi ainsi que de la LIPDA. Il peut toutefois également vérifier la conformité du système par rapport à l'autorisation elle-même. Les pouvoirs du Préposé correspondent à ceux dont il dispose déjà en application de la LIPDA.

Lorsque le Préposé constate que le système de vidéosurveillance ne respecte pas (entièrement ou en partie) les principes, règles et conditions de la loi, de la LIPDA ou de l'autorisation, il peut recommander au responsable du système de modifier ou cesser le traitement découlant de l'utilisation du système. Si le responsable du traitement refuse d'y donner suite, le Préposé peut porter l'affaire par-devant l'autorité compétente pour l'octroi de l'autorisation, en vue d'une décision. Il s'agit là d'un renvoi également à l'article 18 de la loi.

4.18. Article 18

A la suite des compétences de contrôle de l'art. 17, l'article 18 traite de la révocation de l'autorisation ainsi que des voies de droit ouvertes contre une telle décision.

L'alinéa 1 traite des conséquences immédiates du contrôle qui serait effectué par l'autorité compétente ou d'une dénonciation qui lui parviendrait de la part du Préposé (art. 17 al. 2 de la loi). Dès le moment où l'autorité compétente constate que le système de vidéosurveillance ne respecte pas tout ou une partie de l'autorisation ou de la loi (y compris la LIPDA), elle peut enjoindre le responsable du système à s'y conformer dans un certain délai. Si ces irrégularités sont trop importantes, que ce soit en nombre ou dans leurs effets sur les droits des personnes concernées, l'autorité compétente peut ordonner la suspension immédiate de l'autorisation d'exploiter le système. L'autorité requérante devra alors cesser immédiatement toute exploitation et mettre le système hors-service.

L'alinéa 2 traite des suites formelles données au contrôle. Lorsque le système de vidéosurveillance continue à enfreindre les conditions et modalités posées dans l'autorisation, n'y est plus conforme de façon générale ou ne respecte plus les principes de la loi (y compris de la LIPDA), l'autorité compétente peut révoquer son autorisation. L'autorité requérante ne disposera alors plus de l'autorisation d'exploiter le système de vidéosurveillance et devra le mettre immédiatement hors-service ou, en cas de suspension préalable conformément à l'alinéa 1, le conserver hors-service. Afin d'éviter tout abus d'utilisation, le responsable du système devra procéder au démontage des installations de vidéosurveillance au plus vite.

Les voies de droit ouvertes contre la révocation sont précisées à l'alinéa 3. A l'image de ce qui est prévu pour l'autorisation elle-même, la décision de révocation peut faire l'objet d'une réclamation auprès de l'autorité compétente. Ce n'est ensuite que la décision sur réclamation qui est susceptible de recours. Ces deux procédures sont régies par la LPJA, plus précisément les articles 34a ss et 41 ss. Le cercle des personnes disposant d'un moyen de droit contre la décision de révocation est plus restreint que celui applicable à l'autorisation, dans la mesure où seul le responsable du système peut contester la révocation. En dérogation à l'article 34d et 51 LPJA, le projet de loi précise explicitement que la réclamation ainsi que le recours n'ont pas d'effet suspensif. Cela s'impose afin d'éviter que les droits fondamentaux des personnes concernées soient gravement atteints par l'exploitation continue du système non-conforme pendant toute la durée de la procédure.

4.19. Article 19

Le système de vidéosurveillance étant prévu pour s'inscrire dans la durée, des modifications peuvent y être apportées ou découler de son exploitation, éventualité qui est visée par l'article 19.

L'alinéa 1 impose au responsable du système de notifier au Préposé ainsi qu'à l'autorité compétente toute modification substantielle du système préalablement à sa mise en œuvre. Par « substantielle », il convient de comprendre toute modification qui est de nature à porter atteinte aux droits des personnes concernées dans une mesure différente des modalités prévues dans l'autorisation. Tel sera par exemple le cas des modifications qui entraînent l'extension significative de l'horaire d'exploitation des installations de vidéosurveillance, l'ajout de nouvelles caméras, la modification du mode de traitement des données ou l'introduction de nouvelles technologies menant au traitement d'un nombre plus important de données. A l'inverse, ne seront pas substantielles les modifications qui mènent à une réduction de l'horaire d'exploitation des installations de vidéosurveillance ou qui consistent exclusivement en le remplacement des caméras existantes par de nouvelles caméras aux fonctions similaires. Dans tous les cas, toute modification du système doit être reportée dans le rapport établi dans le cadre de l'évaluation annuelle (art. 16 al. 2 de la loi).

L'alinéa 2 autorise l'autorité compétente à adapter l'autorisation en fonction des modifications. Ces modifications (substantielles) et les adaptations doivent toujours respecter les principes et exigences de la loi ainsi que de la LIPDA, dont les principes de l'article 4 et le contenu de l'autorisation selon l'article 13.

4.20. Article 20

L'article 20 constitue la première de deux règles qui visent à assurer une information suffisante entourant le système de vidéosurveillance. Ce premier pan de l'information prend la forme d'une signalisation sur les lieux de la vidéosurveillance.

L'alinéa 1 pose le principe général selon lequel le système de vidéosurveillance doit être signalé par un panneau d'information à l'entrée de la zone concernée. Lorsque les points d'entrée dans la zone ne sont pas clairement limités, par exemple dans le cas d'un parc dont les limites ne sont pas grillagées, des panneaux d'informations doivent être placés aux endroits par lesquels il est « usuel » d'entrer dans la zone, soit essentiellement les chemins d'accès.

Le contenu du panneau est précisé à l'alinéa 2. Il doit informer les passants de l'existence de la vidéosurveillance et du responsable du système. Un moyen simple de contacter le responsable du système doit être mentionné. Il ne serait pas admissible que la personne concernée doive contacter plusieurs personnes au sein de l'administration avant de pouvoir s'adresser à la personne compétente. L'existence de la vidéosurveillance peut être mentionnée par l'utilisation d'un pictogramme reproduisant une caméra de surveillance. Il est renoncé à faire figurer expressément l'existence du droit d'accès.

4.21. Article 21

En tant que deuxième pan de l'information, l'article 21 impose l'existence d'une liste des systèmes de vidéosurveillance soumis à la loi.

L'alinéa 1 charge le Préposé d'établir une telle liste, ce qui suppose de la tenir à jour régulièrement, sur la base des notifications qui lui parviennent selon les articles 14 alinéa 1 (autorisation) et 15 alinéa 3 (vidéosurveillance temporaire) de la loi. Il doit en outre la publier, ce qui peut se faire par le biais du site web du Préposé ou une page *ad hoc* sur le site de l'administration cantonale.

Les informations devant figurer dans la liste tenue par le Préposé sont précisées à l'alinéa 2. Il s'agit en tout cas de la zone surveillée ainsi que du responsable du système et de ses données de contact. Cette énumération n'étant pas exhaustive, le Préposé peut choisir de mentionner d'autres éléments qu'il estimerait pertinents.

4.22. Article 22

L'article 22 traite de deux sujets relatifs au droit transitoire.

D'une part, l'alinéa 1 traite du sort des systèmes de vidéosurveillance déjà en fonction au moment de l'entrée en vigueur du projet de loi. Afin d'octroyer aux autorités les exploitant un certain délai de grâce et éviter une mise hors-service immédiate de l'entier des systèmes déjà en place, la loi prévoit un délai d'une année pour que l'autorité requérante présente une demande et reçoive une autorisation valable pour son système, conformément aux nouvelles dispositions de la présente loi. Cette règle ne s'applique qu'à la condition que (i) le système de vidéosurveillance en question soit déjà en place et exploité au moment de l'entrée en vigueur de la loi et (ii) qu'il était conforme aux réglementations précédemment applicables. A défaut d'une autorisation dans le délai d'une année ainsi prévu, les systèmes de vidéosurveillance doivent être mis hors-service. Si la procédure d'autorisation est en cours, il n'est pas nécessaire de les démonter.

D'autre part, l'alinéa 2 évoque le sort des réglementations communales relatives à la vidéosurveillance qui existent au moment de l'entrée en vigueur de la loi. Une distinction est effectuée dans ce cadre entre les systèmes de vidéosurveillance soumis à l'alinéa 1 (exploités au moment de l'entrée en vigueur de la loi et pour lesquels une autorisation doit être obtenue dans un délai d'une année) et ceux qui ne seraient pas encore exploités. Pour les premiers, les éventuelles réglementations communales existantes à l'entrée en vigueur de la loi demeurent applicables. La seconde phrase de l'alinéa 2 précise toutefois, en dérogation à ce principe, que les règles de la loi relatives à la durée de conservation des images sont applicables immédiatement, rendant inapplicables d'éventuelles dispositions contraires des

réglementations communales. Cette exception est rendue nécessaire par l'atteinte aux droits des personnes concernées que la conservation des images peut entraîner. S'agissant des seconds, ils sont directement soumis aux dispositions de la loi et les dispositions contraires de la réglementation communale seront inapplicables à leur égard. Autrement dit, tout nouveau système de vidéosurveillance ne pourra reposer que sur les règles de la présente loi dès son entrée en vigueur. Cela vise à assurer une application correcte de celle-ci et une uniformité des règles applicables. Formellement en revanche, il appartiendra aux communes d'abroger ces dispositions.

4.23. Article 23

En tant que loi au sens formel, le projet de loi est soumis au référendum facultatif conformément à l'article 31 Cst. VS (alinéa 1). En outre, la date d'entrée en vigueur devra être fixée par le Conseil d'État (alinéa 2).

5. Considérations finales

L'estimation des coûts annuels de fonctionnement du Préposé en particulier au sens des articles 10, 11, 14, 15, 17, 18, 19 et 21 L^{Vid} se montent, selon un honoraire forfaitaire annuel, à fr. 5'000.-

* * *