RAPPORT explicatif
accompagnant l'avant-projet de loi
sur la vidéosurveillance

Le présent rapport explicatif est structuré de la manière suivante :

1. LA MOTION NO 150.06 WEBER-GOBET / STEIERT

Par motion déposée et développée le 15 mai 2006, les députés Marie-Thérèse Weber-Gobet et Jean-François Steiert, avec 22 cosignataires, ont demandé au Conseil d'Etat de présenter au Grand Conseil un projet de loi sur la surveillance vidéo sur le territoire public. A cet égard, ils relèvent que la vidéosurveillance, sous toutes ses formes (surveillance de passages souterrains, de routes, de déchetteries, d'écoles …), comprend généralement un risque d'atteinte grave aux droits fondamentaux protégés par la Constitution, soulevant ainsi d'importantes questions liées à la protection des données et à la protection de la personnalité.

Selon les motionnaires, l'Etat doit se doter d'une loi destinée à donner à la vidéosurveillance un cadre solide et à empêcher tout abus en la matière. Ils estiment insuffisantes les directives non contraignantes de la déléguée cantonale à la protection des données; ils relèvent en outre que la réglementation, sur le plan communal, de cette matière entraîne des inégalités de traitement et constitue un potentiel d'abus important.

La motion no 150.06 a été prise en considération par le Grand Conseil en date du 10 mai 2007. Il appartient dès lors au Conseil d'Etat de présenter au Grand Conseil un projet de loi relatif à la vidéosurveillance sur le territoire public.

2. DEROULEMENT DES TRAVAUX

Le 26 février 2008, le Conseil d'Etat a confié l'élaboration d'un avant-projet de loi sur la vidéosurveillance à un comité de projet formé des personnes suivantes :

M. Thierry Steiert, conseiller scientifique de la Direction de la sécurité et de la justice, président

M. Benoît Rey, conseiller juridique de la Direction de la sécurité et de la justice, chef de projet

Mme Marie-Thérèse Weber-Gobet, députée

M. Christophe Chardonnens, préfet du district de la Broye

M. Charles de Reyff, conseiller communal à Fribourg, représentant de l'Association des communes fribourgeoises

M. Pierre-Alain Sydler, conseiller communal, vice-syndic, Kerzers

Mme Dominique Nouveau Stoffel, préposée à la protection des données

M. Pierre Cottier, Directeur du CO de Bulle

M. Charles Ducrot, adjoint du chef du service des bâtiments

Mme Simone Studer, adjointe du commandant de la Police cantonale

Selon l'organisation du projet approuvée par le Conseil d'Etat, le comité de projet avait pour tâches d'examiner, dans son ensemble, la problématique de la vidéosurveillance (phénomène de la vidéosurveillance en général, état de la situation dans le canton de Fribourg, compétences pour régler la matière) et de préparer un avant-projet de loi pour le Conseil d'Etat.

Le comité de projet s'est réuni à 6 reprises.

3. LA VIDEOSURVEILLANCE - CONSIDERATIONS GENERALES[1]

3.1 Notion

La vidéosurveillance est définie généralement comme la surveillance ou l'observation de personnes ou de biens au moyen de caméras. Elle complète l'observation effectuée par une présence humaine (par ex. par des enseignants, des agents de sécurité ou des concierges). Traditionnellement, l'on distingue la vidéosurveillance d'observation (ou vidéosurveillance simple), sans enregistrement (surveillance de mouvements généraux dans un lieu donné), la vidéosurveillance invasive (surveillance d'une personne à son insu, dans le cadre d'une enquête) et la vidéosurveillance dissuasive. Cette dernière – qui est l'objet principal de l'avant-projet – a pour but d'éviter des atteintes à des personnes ou des biens et à prévenir des infractions. Les données recueillies peuvent servir ensuite de moyens de preuve pour les autorités judiciaires.

Le système de vidéosurveillance est communément constitué de plusieurs dispositifs. Il est composé de caméras (optiques, thermiques ou radar), d'infrastructures de communication et de dispositifs de visualisation, voire d'exploitation d'images. L'exploitation (ou le traitement) d'images consiste notamment à enregistrer les images et à les analyser. Elle peut être effectuée en temps réel ou à posteriori. Les caméras peuvent être fixes ou mobiles, pilotées à distance.

3.2 Intérêts en cause

La vidéosurveillance constitue un outil technologique composant la chaîne de sécurité. Comme déjà dit, elle permet de prévenir, par la dissuasion, des atteintes à des personnes et des biens. Elle sert aussi finalement à identifier les auteurs d'infractions ou d'incivilités. Il est reconnu que la vidéosur-

[1] Certaines de ces considérations sont tirées du Rapport/travaux du CETEL no 55 de l'Université de Genève "vidéosurveillance et risques dans l'espace à usage public, représentation des risques, régulation sociale et liberté de mouvement", Genève octobre 2006

veillance peut apporter un gain organisationnel et peut contribuer à l'action des agents des collectivités sans en multiplier les effectifs.

Cela dit, la vidéosurveillance constitue une forme d'atteinte aux droits fondamentaux constitués par le droit au respect de la vie privée (cf. art. 12 Cst. FR) et la liberté de réunion et de manifestation (cf. art. 24 Cst. FR). La vidéosurveillance constitue aussi une forme particulière de traitement des données personnelles soumise en soi à la législation sur la protection des données (cf. notamment, art. 9 de la loi du 25 novembre 1994 sur la protection des données, LPrD, RSF 17.1). Le traitement des données débute par la collecte des données, il peut se poursuivre, selon les cas, par la conservation, l'exploitation, la communication et la destruction des données recueillies (cf. art. 3 let. d LPrD). La vidéosurveillance doit donc respecter les dispositions de la législation sur la protection des données, destinées à protéger les citoyens contre l'usage abusif des données qui les concernent (cf. art. 12 al. 2 Cst. FR). Les dispositions essentielles sont fixées aux articles 4 à 8 LPrD (notamment : exigence de la base légale et de sécurité, de finalité, de proportionnalité et, enfin, de diligence accrue en cas de collecte de données sensibles). L'exigence de la base légale est essentielle si l'on veut restreindre les droits fondamentaux (cf. art. 38 Cst. FR).

3.3 La réglementation en Suisse

Les législations concernant la vidéosurveillance ne sont pas uniformes en Suisse. La Confédération dispose de bases légales formelles pour la vidéosurveillance de la zone frontalière, des locaux administratifs, des bâtiments du parlement et du gouvernement ainsi que des infrastructures de chemins de fer (cf. le rapport du DFJP sur la vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics, approuvé par le Conseil fédéral le 28 septembre 2007).

Les bases légales cantonales sont encore disparates. Certains cantons réglementent la matière au niveau communal. D'autres ont ancré des dispositions dans les lois sur la police (cf. BE, NW, ZG, AG) ou, plus souvent, dans les lois de protection des données (SZ, OW, GL, BS, AG, GE, NE, VD). Plusieurs cantons n'ont encore aucune disposition légale spéciale, se contentant de recommandations de leurs autorités cantonales de surveillance en matière de protection des données (cf. ZH, LU, SO, BL, TI). Le canton de Fribourg est actuellement dans cette situation (cf. l'aide mémoire no 6 de la surveillance vidéo édicté par l'Autorité cantonale de surveillance en matière de protection des données).

3.4 La situation en fait à Fribourg

Une enquête a été effectuée par le comité de projet en mars 2008 dans le canton de Fribourg. Lors de cette enquête, plusieurs autorités ont été abordées, qui utilisent ou auraient pu utiliser des systèmes de vidéosurveillance. L'enquête a porté sur divers points (endroits concernés, buts recherchés, systèmes utilisés, personnes autorisées à visionner les images, délai de destruction du matériel recueilli, etc.). Le rapport d'évaluation de cette enquête a montré d'abord que plusieurs autorités utilisaient déjà des dispositifs de vidéosurveillance (certains collèges, services « sensibles », tribunaux etc.), et ce dans le but surtout de prévenir les atteintes à des personnes et des biens. L'enquête a aussi révélé que les délais de destruction du matériel recueilli étaient des plus divers (24 h à 30 jours !) et que l'information des personnes visionnées n'était pas toujours assurée. Cela dit, plusieurs autorités ont estimé que la vidéosurveillance était inutile, estimant la présence humaine préférable (concierges, agents de sécurité, …); d'autres l'ont estimé inutile en l'état au vu du peu d'infractions commises. S'agissant des bases légales, les autorités concernées appliquent en général l'aide mé-

moire no 6 de la surveillance vidéo édicté par l'Autorité cantonale de surveillance en matière de protection des données, ou des directives particulières internes.

4. L'AVANT-PROJET DE LOI SUR LA VIDEOSURVEILLANCE

4.1 Ancrage de la matière

L'avant-projet met en œuvre la motion des députés Marie-Thérèse Weber-Gobet et Jean-François Steiert, prise en considération le 10 mai 2007.

Le comité de projet s'est tout d'abord penché sur une question d'ordre formel : faut-il ancrer la matière dans la loi sur la protection des données (comme bon nombre de cantons l'ont fait) ou prévoir une loi spéciale ? Le comité de projet a opté pour cette dernière solution, qui a l'avantage d'être claire et qui offre une meilleure visibilité. Le but de la réglementation est avant tout de déterminer quand une récolte de données par vidéosurveillance est licite (principe de l'intérêt public, allié à celui de proportionnalité). De telles dispositions, précisant les conditions générales de licéité du traitement, méritent une assise légale particulière.

4.2 Dispositif de contrôle envisagé

En ce qui concerne la réglementation du contrôle (préventif) de la vidéosurveillance, deux solutions sont envisageables: soit la collectivité publique informe (préalablement) l'autorité compétente de la mise en place de l'installation, soit elle doit requérir auprès de cette autorité une autorisation formelle préalable. Le comité de projet a opté pour ce dernier système, jugé plus clair et efficace. Un simple système d'information, même préalable à la pose de l'installation, ne serait pas assez strict ; il empêcherait une appréciation claire de l'autorité portant sur la réalisation des conditions exigées par la loi. Certes, un système simple d'information pourrait s'intégrer dans le nouveau dispositif d'intervention de l'autorité de surveillance cantonale, prévu dans le nouvel article 22a LPrD. Rappelons que ce nouveau dispositif prévoit un système de recommandations de l'autorité de surveillance suivi de décisions de l'organe responsable, pouvant finalement aboutir à un recours de l'autorité de surveillance auprès du Tribunal cantonal. Ce système n'a cependant pas été jugé satisfaisant pour répondre aux besoins en matière de vidéosurveillance. C'est donc un système plus formel d'autorisation qui est proposé, avec conditions et modalités, mis en œuvre par une procédure décisionnelle ordinaire, avec voie de droit, conformément au code de procédure et de juridiction administrative (CPJA) (cf. art. 3ss AP).

4.3 Commentaire des dispositions

Article premier

Cet article fixe l'objet et les buts de la loi. L'alinéa 1 est une disposition axiale : il fixe le but de la vidéosurveillance, qui est double : préventif et répressif. L'alinéa 3 montre l'ancrage de la loi spéciale dans le système général prévu par la loi sur la protection des données. Sous cet angle, la loi spéciale précise les conditions et les modalités essentielles liées au traitement des données (cf. art. 4 à 13 LPrD) en introduisant un système d'autorisation et d'information, avec la compétence d'une autorité cantonale spécialement désignée, le préfet (cf. art. 3ss AP). La législation sur la protection des données s'appliquera ainsi pour tout ce qui n'est pas réglé par la loi spéciale, notamment pour ce qui concerne la communication des données (cf. art. 10 à 12 LPrD), les droits des personnes concernées (cf. art. 23 à 28 LPrD) et la surveillance générale (cf. art. 29 à 32 LPrD).

L'alinéa 2 définit ce que l'on entend par vidéosurveillance au sens de la loi (cf. aussi ch. 3.1 ci-dessus). L'avant-projet ne vise que la surveillance de personnes ou de biens au moyen de caméras; il ne vise pas la surveillance par d'autres moyens (cf. par ex., un contrôle d'entrée par des rayons-X ou par la perception de la chaleur). Ces installations peuvent être placées de façon provisoire ou définitive.

Article 2

Conformément au mandat donné par le Grand Conseil, le champ d'application personnel de la loi couvre les collectivités publiques et les personnes privées qui accomplissent des tâches de droit public (cf. art. 2 al. 1 let. a et b AP). Sous cet angle, le champ d'application personnel est identique à celui de la loi sur la protection des données (cf. art.2 al.1 LPrD). Ce champ d'application personnel est cependant étendu aux personnes privées qui mettent en place des dispositifs portant en tout ou en partie sur le domaine public (cf. art. 2 al. 1 let. c). Cette extension se justifie car le domaine public est touché. En revanche, l'avant-projet ne règle pas la vidéosurveillance de personnes privées sur leur domaine privé, quand bien même celui-ci serait ouvert au public (cf. par ex. les installations dans les galeries marchandes ou la vidéosurveillance à l'intérieur d'une banque). La loi fédérale sur la protection des données s'applique à de telles situations.

Le champ d'application matériel est circonscrit au « territoire public », c'est-à-dire au domaine public cantonal ou communal au sens de la loi du 4 février 1972 sur le domaine public (LDP ; RSF 750.1). Cela dit, pour ce qui est des immeubles affectés à l'administration publique (par ex., hôpitaux, écoles, bâtiments administratifs, …), seuls sont visés par la loi les immeubles ou parties d'immeubles ouverts au public (accessibles au public). Cette restriction s'impose car la surveillance effectuée dans les locaux administratifs non ouverts au public (par ex., quartiers cellulaires dans les prisons, chambres d'hôpitaux etc.) obéit à d'autres règles et ne peut être soumise aux mêmes restrictions que la vidéosurveillance dans les endroits accessibles au public. Concrètement, le champ d'application matériel vise les endroits suivants :

- les immeubles affectés à l'administration publique et ouvert au public
- les choses affectées, par le fait ou par décision, à l'usage commun et aménagées à cet fin, tels les routes, les places, les parcs, de manière générale les voies de communication et ouvrages annexes.
- les choses destinées par nature à l'usage commun, en particulier des eaux publiques

En soi, les biens du patrimoine financier (privé) des collectivités (par ex. des immeubles locatifs ou des vignes appartenant à des collectivités publiques) ne tombent pas dans le champ d'application matériel de l'avant-projet. La vidéosurveillance de ces biens est exclusivement régie par la loi fédérale sur la protection des données, les collectivités publiques agissant ici comme propriétaires privés.

La vidéosurveillance effectuée dans le cadre d'enquêtes pénales est aussi exclue du champ d'application de l'avant-projet (cf. art. 134 al. 4 et 150 al. 1 let. b du code de procédure pénale du 14 novembre 1996 ; CPP ; art. 280 et 281 du code de procédure pénale suisse du 5 octobre 2007). Cette exclusion ne vaut que si la vidéosurveillance est ordonnée par la Police cantonale ou un juge. Cela dit, est aussi exclue du champ d'application la vidéosurveillance (d'observation essentiellement) mise en place par la Police cantonale, hors procédure pénale, pour pouvoir accomplir ses tâches (cf. art. 38b LPol et art. 41 LPol).

Article 3

L'avant-projet propose un système d'autorisation, accordée à l'organe responsable de la collectivité publique concernée ou à la personne privée concernée. L'organe public sera celui qui est responsable de la protection des données (cf. art. 17 LPrD). En général, cet organe sera, au niveau de l'Etat, soit le Service des bâtiments chargé de gérer les bâtiments du domaine public cantonal, soit le Service des ponts et chaussées; mais il pourra aussi s'agir, selon la législation applicable, des organes d'établissements publics autonomes. Au niveau communal, l'organe responsable sera le conseil communal, cas échéant un comité d'association de communes.

L'avant-projet prévoit que l'autorité compétente pour décider soit le préfet, magistrat élu, responsable de façon générale de l'ordre et de la sécurité publics dans son district. Cette autorité a été choisie car le but de la vidéosurveillance est bien lié à l'ordre et à la sécurité publics. Le préavis de l'Autorité cantonale de surveillance en matière de protection des données sera requis pour chaque procédure d'autorisation.

Article 4

Cet article fixe les conditions d'octroi de l'autorisation. Ces conditions découlent des dispositions des articles 5 à 9 LPrD exposant les principes généraux de finalité et de proportionnalité. Le critère exposé à l'article 4 al. 1 let. c AP a été introduit en précision de l'article 9 al. 2 LPrD, lequel ne fait que disposer que la récolte de données doit être reconnaissable comme telle. L'information sera donnée à l'endroit même où la prise d'images a lieu ; elle sera limitée à l'existence de la vidéosurveillance (par la pose d'un sigle ou d'un pictogramme, éventuellement d'un texte).

Article 5

Cet article fixe les modalités de la vidéosurveillance.

En ce qui concerne le délai pour la destruction des images enregistrées, les pratiques et les règlements existants en Suisse sont très disparates. L'avant-projet propose un délai qui est suffisant pour que la personne qui visionne les images soit en mesure de réagir (information donnée à son supérieur ; dénonciation pénale, …). Sous cet angle, un délai maximal de 7 jours semble adéquat. Si des informations sont recueillies, démontrant des atteintes à des personnes ou des biens, ce délai peut être porté à 100 jours au maximum. Un tel délai, jugé admissible par le Tribunal fédéral, est suffisant pour que la collectivité puisse réagir et prendre le cas échéant la décision de dénoncer pénalement les comportements visionnés. IL convient de rappeler que ces délais sont indépendants de ceux imposés aux autorités judiciaires (cf. délais de conservation de pièces judiciaires, liés à la prescription de l'action pénale).

Les autres modalités consistent pour l'essentiel en la prise de mesures de sécurité suffisantes (cf. art. 5 al. 2 AP). Cette exigence est déjà concrétisée par des dispositions spéciales contenues dans le règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15). Ce règlement porte notamment sur la protection des données recueillies contre tout traitement non autorisé et sur les exigences concernant les personnes autorisées à accéder aux informations (cf. art. 3 et 10 RSD).

Le règlement d'utilisation constitue une exigence essentielle (cf. art. 5 al. 3 AP). L'autorité compétente recevra ce règlement avec la requête d'autorisation et, par la suite, lors de chaque modification du système (par ex. modification de la localisation, de l'installation technique, de l'information donnée ou des délais de destruction) (cf. art. 5 al. 4 AP). Le Conseil d'Etat précisera le contenu de ce règlement d'utilisation (cf. art. 3 al. 4 AP).

A remarquer que le système d'autorisation prévu ne supprime pas le contrôle hiérarchique prévu par l'article 25 du règlement sur la sécurité des données personnelles. Seule l'autorité hiérarchique est habilitée à procéder au contrôle de l'existence de mesures de sécurité et techniques nécessaires, le contrôle de l'Autorité de surveillance en matière de protection des données étant réservé (cf. art. 26 du règlement précité). Le préfet n'exercerait en la matière aucune compétence.

Article 6

Cet article contient les dispositions habituelles relatives au retrait des autorisations.

Article 7

Cet article introduit une obligation d'information pour les organes publics et les personnes privées qui veulent mettre en place une vidéosurveillance dite d'observation (vidéosurveillance simple), sans enregistrement (cf. par ex. : webcam dans une ville, surveillance d'un tunnel routier).

Le comité de projet estime que cette forme de surveillance n'a pas à être soumise à un système d'autorisation. Aucun enregistrement n'est effectué, de sorte que la violation des droits fondamentaux est en soi inexistante (la Cour européenne des droits de l'Homme avait jugé dans ce sens le 17 juillet 2003, cf. le Rapport du CETEL no 55, ch. 6.2.1). Cela dit, la mise en place d'une telle vidéosurveillance créée un risque d'atteinte, surtout si le dispositif permet l'identification de personnes. C'est précisément pour permettre à l'autorité de vérifier ces éléments que l'avant-projet prévoit un simple système d'information.

La violation de cette obligation par des personnes privées entraînera les mesures prévues à l'article 8 de l'avant-projet. Pour les organes publics, le dispositif prévu par la loi sur la protection des données s'appliquera (cf. la procédure de recommandation / décision exposée à l'art. 22a LPrD).

Article 8

Cet article prévoit des dispositions pénales spéciales lorsque des personnes privées (cf. art. 2 al. 1 let. b et c AP) violent certaines dispositions de la loi. La compétence pour infliger des amendes est prévue par le code de procédure pénale (compétence du juge de police ou du juge d'instruction). A remarquer que l'avant-projet renonce à confier principalement au préfet cette compétence. En effet, celui-ci devra se récuser s'il a traité de l'affaire sous l'angle administratif par ex. s'il a traité auparavant l'autorisation accordée à la personne privée dont l'installation portait sur le domaine public (cf. art. 53 let. c de la loi d'organisation judiciaire). Il est bien évident que ces dispositions pénales ne concernent que les personnes privées, à l'exclusion des collectivités publiques, qui ne peuvent pas être condamnées pénalement.

Article 9

Cet article contient une disposition modificatrice de la loi du 25 novembre 1994 (RSF 17.1) sur la protection des données. Une réserve de la loi sur la vidéosurveillance s'impose en effet dans la loi générale sur la protection des données (cf. art. 2 al. 4 LPrD, tel que proposé). La LPrD s'appliquera pour tout ce qui n'est pas réglé par la loi sur la vidéosurveillance (cf. art. 1 al. 3 in fine AP et le commentaire ci-dessus y relatif).

Article 10

Des dispositions transitoires s'imposent pour octroyer un délai aux personnes et aux collectivités publiques soumises à la loi, afin que celles-ci puissent se mettre en conformité avec le nouveau régime légal.

5. INCIDENCES

L'avant-projet n'a pas d'incidences sur la répartition des tâches entre l'Etat et les communes.

L'avant-projet est conforme à la Constitution cantonale (cf. art. 12, 24 et 38 Cst. FR) et à la Constitution fédérale. Il est par ailleurs conforme au droit européen en matière de protection des données (directive 95/46/CE et convention 108, y compris son protocole additionnel).

Les dispositions de l'avant-projet, en particulier celles concernant le système d'autorisation et d'information, introduisent de nouvelles tâches pour les préfets (autorité compétente au fond) et pour l'Autorité cantonale de surveillance en matière de protection des données (autorité de préavis et de surveillance générale). Il ne sera cependant vraisemblablement pas nécessaire de renforcer les effectifs des autorités compétentes en raison de cette nouvelle législation. En outre, des émoluments pourront être perçus, fixés par le Conseil d'Etat, à la charge des collectivités publiques et des personnes privées soumises à la loi.