ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

SURVEILLANCE VIDÉO

Aide-mémoire concernant la surveillance vidéo effectuée par des organes publics cantonaux et communaux dans des lieux et bâtiments publics.

1. Objectif

Le présent aide-mémoire se fonde sur le pouvoir de conseil de la Préposée (art. 31 al.2 let. b de la Loi du 25 novembre 1994 sur la protection des données, LPrD). A considérer comme ligne de conduite, il a pour but de guider les organes publics cantonaux ou communaux compétents lorsqu'ils veulent installer un système de caméras de surveillance pour assurer la sécurité à l'intérieur et aux abords des lieux et bâtiments publics.

2. Généralités

Voici d'abord quelques informations générales.

2.1 Au sens de la protection des données, on entend par **surveillance vidéo** la prise d'images se rapportant à des *personnes* reconnaissables ou identifiables. Les traitements effectués sont notamment capter, transférer, visionner en direct ou à posteriori, enregistrer et conserver les images.

2.2 La surveillance vidéo concernant les personnes constitue une *atteinte importante* au droit constitutionnel fondamental à la **vie privée** (art. 12 Constitution du canton de Fribourg du 16 mai 2004). L'atteinte à la personnalité se concrétise lorsque les images de personnes reconnaissables ou identifiables sont traitées, voire enregistrés. Par ce biais, il est alors possible de constituer des profils de personnalité et de mouvements;
le risque d'atteinte à la personnalité est autant plus grand que les moyens techniques deviennent toujours plus raffinés (par ex. des caméras web, braquées sur les lieux publics, fournissent en direct sur internet des images qui peuvent être traitées sans aucun contrôle).

2.3 Le fait d'être surveillé peut inciter les personnes à modifier leur comportement habituel, ce qui porte atteinte au droit constitutionnel fondamental à la **liberté personnelle** (art. 11 al. 2 Constitution du canton de Fribourg du 16 mai 2004).

2.4 La surveillance vidéo suscite des controverses à cause de sa **« sécurité factice »**.
Les personnes dans la zone surveillée peuvent se croire en sécurité et par conséquent se comporter moins prudemment; si les images ne sont pas observées en direct et que personne ne peut intervenir en cas d'urgence, le sentiment de sécurité peut être trompeur.

3. Conditions préliminaires à la mise en place d'une surveillance vidéo
Les organes publics qui recourent à la surveillance vidéo sont tenus de prendre toutes les dispositions nécessaires pour prévenir le risque accru d'atteinte à la personnalité. Par conséquent, la surveillance vidéo doit être limitée aux cas où des mesures moins radicales ne permettent pas d'atteindre le but recherché.

3.1 L'installation d'une surveillance vidéo nécessite une **analyse préalable** *des risques* et *des mesures possibles* eu égard au but poursuivi. Il faut examiner les moyens actuels, les avantages et désavantages de la surveillance vidéo et déterminer son but précis. En particulier, il faut se poser les questions suivantes :

a) quant à l'*analyse des risques* : y a-t-il eu des atteintes contre des personnes ou des biens dans des lieux à protéger ou y a-t-il un danger concret que ces atteintes se produisent ?

b) quant aux moyens : quels sont les *moyens actuels* et quels seraient les moyens possibles et moins radicaux que la surveillance vidéo (par ex. verrouillages complémentaires, renforcement des portes, système d'alarme) ?

c) quant au *but* de la surveillance vidéo, il doit être précisé : si le but est de protéger la vie, l'intégrité physique et sexuelle des personnes dans un garage souterrain, la surveillance doit être effectuée en direct et il doit avoir une possibilité d'intervention immédiate dans le cas d'urgence; si le but est de protéger un bâtiment contre le vandalisme, une surveillance à posteriori pourrait suffire en raison de l'effet préventif de la présence d'une caméra.

3.2 L'**Autorité de surveillance** en matière de la protection des données peut être consultée durant le processus examinant la question de la mise en place d'un système de surveillance vidéo (par ex. sur la nécessité d'établir un concept, sur les modalités, art. 31 al. 2 let. b LPrD). Après l'installation d'une caméra vidéo, l'Autorité de surveillance a la possibilité d'effectuer des contrôles dans le cadre de ses compétences (art. 31 al. 2 let. a LPrD).

4. Exigences juridiques à l'autorisation d'un système de surveillance vidéo
Il s'agit d'examiner si les conditions nécessaires sont remplies pour qu'un système de surveillance vidéo puisse être autorisé par l'organe public. À ce stade, les principes juridiques suivants sont à respecter :

4.1 Il faut une **base légale** au sens formel qui précise les points suivants :

a) l'*objectif* de la surveillance vidéo (qui lui-même doit aussi être licite : par ex. une installation pour l'observation du comportement des employés par l'employeur est interdite par la loi);

b) les personnes *autorisées à gérer* la surveillance vidéo;

c) les personnes *autorisées à consulter* les images et les circonstances qui leur permettent de le faire;

d) l'*objet* surveillé (bâtiments, transports publics, des déchetteries, autres lieux etc.) et les temps (durées) de la surveillance vidéo;

e) la possibilité d'*enregistrer* les images, et cas échéant, la *durée* d'enregistrement.

4.2 Il faut assurer le respect du principe de la **proportionnalité** de la façon suivante :

a) Le *but à atteindre* doit être adapté à cette mesure et donc d'une importance élevée (par ex. protéger la vie et l'intégrité physique des personnes, combattre le vandalisme; la surveillance par caméra d'une déchetterie ou d'un tunnel souterrain pour les piétons est discutable);
b) la surveillance doit être *adéquate*, c'est-à-dire apte à atteindre le but poursuivi, et elle doit être limitée à ce qui est nécessaire; par ex. si le but est de protéger des personnes dans un garage souterrain, la surveillance doit être effectuée en direct et il doit avoir une possibilité d'intervention immédiate dans les cas d'urgence; visionner les images à posteriori ne suffirait pas dans ce cas ; d'autre part, il faut renoncer à la surveillance vidéo si d'autres mesures moins invasives (par ex. un système d'alarme etc.) s'avèrent suffisantes et praticables.

5. Exigences juridiques en cas d'installation et d'utilisation d'un système de surveillance vidéo

Si les conditions pour l'autorisation d'une surveillance vidéo sont remplies, il faut examiner la prochaine étape. Cela veut dire que, dès la mise en service d'une caméra de surveillance, les principes juridiques en matière de la protection des données indiqués ci-après doivent être respectés.

5.1 Il convient de mettre en place les mesures pour assurer les principes de la **transparence** et de la **bonne foi**, ainsi que l'exercice des **droits des personnes concernées** :

a) les caméras doivent être installées à un endroit *visible*; si nécessaire, il faudra les protéger contre le vandalisme (par ex. par une grille protectrice);

b) le responsable de la surveillance vidéo doit *informer* les personnes qui se trouvent dans la zone surveillée qu'un système de surveillance vidéo y est installé (par ex. par un panneau visible et lisible); cet avis doit fournir les informations principales (le but et le champ de la surveillance, le fait que les personnes peuvent être reconnues et identifiées par la caméra, les périodes de fonctionnement, le responsable, l'enregistrement des prises de vue et, le cas échéant, la durée de l'enregistrement);

c) les *droits* des personnes concernées doivent être prévus par le système; l'avis doit aussi indiquer auprès de qui le droit d'accès peut être exercé.

5.2 Pour respecter le principe de la **finalité**, il faut garantir ce qui suit :

a) les images filmées ne peuvent être utilisées que dans le *but déclaré* ou découlant des circonstances (par ex. : si une caméra, installée dans un garage souterrain pour empêcher les atteintes aux personnes, capte par hasard des élèves fumant un joint, ces images ne peuvent pas être utilisés);

b) les données ne peuvent pas être transmises ou vendues à un tiers; la *communication* des données enregistrées est interdite sauf dans les cas prévus par la loi.

5.3 Pour tenir compte du principe de la **proportionnalité**, il faut que :

a) la caméra ne surveille que la *zone absolument nécessaire* pour atteindre le but prévu (par ex. la caméra, dont le but est de protéger une école contre le vandalisme, doit viser les murs du bâtiment et pas l'espace entier autour de l'école); les personnes non concernées doivent avoir la possibilité d'éviter le champ de la caméra (pas de « passage obligé », pas de surveillance vidéo « totale »);

b) la caméra ne soit pas dirigée sur des endroits tels que des maisons privées, des fenêtres d'immeubles, salles de bain, de toilettes ou d'essayage, chambres d'un hôpital, etc. afin de *respecter la sphère privée* de l'individu;

c) la caméra soit active seulement pendant le *temps nécessaire* pour atteindre le but (par ex. : la caméra qui surveille un passage souterrain pour piétons très fréquenté pendant la journée fonctionnera uniquement durant la nuit);

d) l'organe public vérifie régulièrement si la surveillance est *encore nécessaire* et mette fin à la surveillance si l'objectif est atteint.

5.4 En ce qui concerne la **sécurité des données**, le responsable du système doit prendre les mesures organisationnelles et techniques appropriées afin de protéger les données personnelles contre tout traitement non autorisé (par ex. visionnement ou manipulation des images), par ex. :

a) seules les personnes *autorisées* peuvent avoir accès aux écrans des caméras.

b) les enregistrements doivent être *conservés* en un endroit sûr et un local fermé;

c) le personnel traitant ces données doit être *instruit* de façon adéquate, *surveillé* et *contrôlé* par rapport au respect des mesures de sécurité et de protection des données.

5.5 Il convient en matière de **technologies** :

a) d'utiliser des *technologies favorables* à la protection des données (par ex. des « privacy filters » qui reconnaissent et brouillent les visages filmés en direct, en respectant ainsi la sphère privée des personnes non concernées qui se trouvent dans le secteur surveillé; si les enregistrements sont nécessaires à l'identification d'une personne – par ex. lors d'une procédure pénale – le brouillage peut être enlevé);

b) de renoncer aux *caméras-attrapes* : leur utilisation est à déconseiller parce que ces attrapes trompent les personnes concernées et violent ainsi les règles de la bonne foi; en tout état de cause elles sont soumises aux mêmes conditions que les caméras effectives.

5.6 Finalement, quant à la **conservation** et à la **destruction** des images :

a) s'il s'agit d'une surveillance *en direct* (observation sur un moniteur), un enregistrement n'est pas nécessaire et donc pas admissible sauf en cas d'une atteinte observée à des personnes ou à des biens.
b) s'il s'agit d'une surveillance *indirecte* (à posteriori), les données enregistrées doivent être effacées au plus vite, par ex. 24 heures après l'enregistrement et si aucun événement n'a été constaté dans ce délai.

N.B. Les images constatant une atteinte ne peuvent être *transmises* qu'à l'organe compétent de poursuite pénale (police, juge, etc.) et il n'est pas admissible d'en garder des copies.

Fribourg, avril 2005