

POSTULAT N° 102 (2011-2016)
RAPPORT FINAL

EXTRAIT DU PROCES-VERBAL
DE LA SEANCE DU CONSEIL GENERAL
DU 16 DECEMBRE 2014

M. Pierre-Alain Clément, Syndic, présente le rapport ci-après:

"En séance du 1^{er} octobre 2013, le Conseil général transmettait au Conseil communal le postulat n° 102 de Mme B. Acklin Zimmermann et de M. J.-P. Wolhauser, ainsi que de 18 cosignataires, lui demandant d'intervenir auprès du Préposé fédéral à la protection des données et à la transparence (PFPDT) pour que chaque installation de vidéosurveillance soit clairement signalisée dès l'entrée du bâtiment.

Les auteurs relèvent que de nombreux commerces de la ville de Fribourg sont équipés d'un système de vidéosurveillance. Une partie d'entre eux ne signale pas à leurs clients qu'ils sont filmés. Il s'agit d'un procédé illégal, contraire à la loi fédérale sur la protection des données.

Réponse du Conseil communal

1. Généralités

L'utilisation, par des particuliers, de caméras vidéo à des fins de protection des personnes ou de prévention d'actes de vandalisme tombe sous la loi fédérale sur la protection des données (LPD; RS 235.1) lorsque les images tournées montrent des personnes identifiées ou identifiables. Ce principe vaut indépendamment du fait que les images sont conservées ou non. Le traitement des images – collecte, communication, visionnement immédiat ou différé, conservation – doit satisfaire aux principes généraux de la protection des données. L'utilisation de la vidéosurveillance sur le domaine privé n'est toutefois pas soumise à autorisation.

L'exploitation d'un système de vidéosurveillance implique le traitement permanent de données personnelles. Cette forme de surveillance peut en outre, en fonction de la situation, porter sensiblement atteinte à la sphère privée des personnes filmées. Il importe par conséquent d'accorder une attention particulière aux règles de la protection de la personnalité lors de la planification, de l'installation et de l'exploitation de tels systèmes. Les systèmes de vidéosurveillance ne sont autorisés qu'à condition qu'ils respectent les principes de licéité et de proportionnalité (article 4 LPD). Chaque système de vidéosurveillance doit concrètement remplir les conditions suivantes:

- a. La vidéosurveillance ne peut être effectuée que si les personnes filmées ou susceptibles de l'être y consentent ou si l'atteinte à la personnalité qu'elle représente est justifiée par un intérêt prépondérant, public ou privé, ou par la loi (principe de la licéité, article 4 alinéa 1 LPD). Dans la pratique, il est généralement impossible de demander leur accord à toutes les personnes filmées pour exploiter un système de vidéosurveillance. Dans le doute, la vidéosurveillance ne doit être effectuée que s'il existe un intérêt privé ou public prépondérant, donc à des fins de sécurité.
- b. La vidéosurveillance doit être un moyen adéquat de réaliser le but poursuivi, à savoir la sécurité (notamment la protection contre les atteintes aux personnes ou aux biens). Elle ne peut être pratiquée que si d'autres mesures moins attentatoires à la vie privée, telles que des verrouillages complémentaires, le renforcement des portes d'entrée ou des systèmes d'alarme, s'avèrent insuffisantes ou impraticables. En outre, les atteintes à la sphère privée causées par la vidéosurveillance doivent se trouver dans un rapport proportionné par rapport au but visé (principe de la proportionnalité, article 4 alinéa 2 LPD).

2. Installation d'un système de vidéosurveillance

Le système de vidéosurveillance doit être installé de telle manière que les principes de la proportionnalité, de la bonne foi et de la transparence sont respectés:

- a. *La caméra doit être installée de manière que n'entrent dans son champ que les images strictement conformes au but de la surveillance (principe de la proportionnalité).*
- b. *En règle générale, une surveillance vidéo effectuée à des fins privées n'est possible que dans le propre terrain. La surveillance vidéo de l'espace public relève de la législation cantonale.*
- c. *Le responsable du système de vidéosurveillance doit informer les personnes entrant dans le champ des caméras de l'utilisation d'un tel système au moyen d'un avis bien visible. Au cas où les images sont enregistrées sous quelque forme que ce soit, l'avis doit également indiquer auprès de qui les personnes filmées peuvent faire valoir leur droit d'accès si cela ne ressort pas du contexte (principe de la bonne foi et droit d'accès).*

3. Principes à respecter lors de l'exploitation d'un système de vidéosurveillance

- a. *Les données ne peuvent être utilisées que dans le cadre de la protection contre les atteintes aux personnes ou aux biens. Elles ne peuvent donner lieu à d'autres utilisations (principe de la finalité). Ainsi, un centre commercial ne peut pas utiliser à des fins de marketing les images filmées par une caméra vidéo installée dans le but d'assurer la sécurité.*
- b. *Le responsable du système de vidéosurveillance doit prendre les mesures organisationnelles et techniques appropriées pour protéger les données personnelles contre tout traitement non autorisé (sécurité des données, article 7 LPD). Lorsque les images sont transmises par radiocommunication de la caméra au lieu d'enregistrement, le signal doit être crypté ou protégé par d'autres mesures adéquates à même de garantir que des personnes non autorisées ne puissent pas intercepter le signal et visionner les images.*
- c. *Le nombre des personnes qui ont accès aux images - que celles-ci soient diffusées en direct ou enregistrées - doit être aussi restreint que possible (sécurité des données et proportionnalité). Les écrans d'un système de vidéosurveillance doivent être tournés de manière que seul le personnel autorisé peut voir les images. Les écrans publics sont proscrits. Il faut en outre déterminer si le but poursuivi par la vidéosurveillance requiert une surveillance en direct ou s'il suffit que les données vidéo enregistrées soient évaluées suite à un événement. Si la seconde option prévaut, les images ne peuvent être visionnées qu'après un événement le justifiant.*
- d. *Les données personnelles enregistrées ne doivent pas être divulguées, sauf si les images sont remises à des fins de dénonciation aux autorités de poursuite pénale ou dans des cas prévus ou autorisés par la loi; par exemple, lorsqu'un juge en fait la demande (principe de la finalité).*
- e. *Les données personnelles enregistrées par une caméra doivent être effacées dans un délai particulièrement bref. En effet, la constatation d'une infraction aux personnes ou aux biens aura lieu, dans la plupart des cas, dans les heures qui suivent sa perpétration. Un délai de 24 heures apparaît donc suffisant au regard de la finalité poursuivie, pour autant qu'aucune atteinte aux personnes ou aux biens ne soit constatée dans ce délai. Lorsque des motifs objectifs et importants justifient une durée de conservation plus longue, la durée peut être prolongée en conséquence. En outre, la durée peut être plus longue s'agissant de la vidéosurveillance de locaux privés non accessibles au public (principe de la proportionnalité). Plus les images sont conservées longtemps, plus les exigences en matière de sécurité des données sont élevées. Toute prolongation de la durée de conservation doit être compensée par l'utilisation de technologies permettant de protéger les données (par exemple brouillage) et par le cryptage des images enregistrées.*
- f. *Le responsable du système de vidéosurveillance doit, lorsqu'elles le demandent, renseigner toutes les personnes entrées dans le champ de la caméra sur les images les concernant.*

4. Autorité compétente

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) accomplit notamment les tâches suivantes:

- *surveillance des organes fédéraux (art 27 LPD);*
- *conseil aux personnes privées (article 28 LPD);*
- *surveillance des personnes privées (article 29 LPD);*
- *information du public (article 30 alinéa2 LPD).*

Selon l'article 28 LPD, le préposé conseille les personnes privées en matière de protection des données. Quant à l'article 29 LPD, il dispose que le préposé établit les faits d'office ou à la demande de tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système); des fichiers doivent être enregistrés (article 11a LPD); il existe un devoir d'information au sens de l'article 6 alinéa 3 LPD. Sur la base de ses constatations, il peut ensuite émettre des recommandations.

A la suite du dépôt du postulat, le Service juridique de la Ville de Fribourg a pris contact avec le PFPDT concernant cette problématique. Selon le PFPDT, seules les personnes privées peuvent saisir le PFPDT.

Comme il s'agit d'une affaire civile (articles 28 à 28I CC), une commune ne peut ni se substituer à un particulier, ni demander au PFPDT d'intervenir de manière générale dans tous les commerces fribourgeois qui ne respectent pas la législation fédérale sur la protection des données. Si tant est qu'elle soit possible, une intervention limitée à un rappel de l'obligation de signaler la vidéosurveillance ne réglerait que très partiellement la problématique de la protection des données personnelles qui ne se limite pas à ce seul aspect. Comme le relève le PFDPT, il appartient avant tout aux particuliers d'exiger le respect des droits que la loi a aménagé pour les particuliers (cf. PFPDT, Droits de la personne concernée en matière de traitement des données personnelles, Berne, mai 2014).

A cet effet, le particulier peut, dans un cas d'espèce:

- *s'adresser au PFPDT pour obtenir des conseils (article 28 LPD);*
- *s'adresser au responsable de la vidéosurveillance (article 8 LPD); un formulaire est disponible sur le site internet du PFPDT (<http://www.edoeb.admin.ch/>);*
- *intenter une action civile (article 15 LPD)."*