



ETAT DE FRIBOURG
STAAT FREIBURG

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

La Préposée cantonale à la protection des données

Rue des Chanoines 2, 1700 Fribourg

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

—
Réf. : dossier 8041 DNS/GG

PRÉAVIS
du 3 octobre 2012

À l'attention du Préfet de la Sarine, M. Carl-Alex Ridoré

Demande d'autorisation d'installation de vidéosurveillance

Office de la Circulation et de la navigation (ci-après : OCN), route de Tavel 10, case postale 192, 1707 Fribourg

I. Généralités

Vu

- les art. 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst RSF ; 10.1) ;
- l'art. 5 al. 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'art. 5 al. 1 de l'Ordonnance cantonale du 23 août 2011 sur la vidéosurveillance (OVid ; RSF 17.31) ;
- la Loi cantonale du 25 novembre 1994 sur la protection des données (LPrD ; RSF 17.1) ;
- le Règlement du 29 juin 1999 sur la sécurité des données personnelles (RSD ; RSF 17.15),

l'Autorité cantonale de la transparence et de la protection des données formule le présent préavis concernant la requête de l'OCN visant à l'installation d'un système de vidéosurveillance avec enregistrement, comprenant cinq caméras de marque Siemens, dôme avec zoom, montage apparent, liaison par câble, enregistrement sur serveur dédié, fonctionnant 24h/24.

Ce préavis se base sur les éléments qui ressortent du formulaire de demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement daté du 21 août 2012 et de son Règlement d'utilisation (Annexe), transmis par la Préfecture de la Sarine par courrier du 30 août 2012. Le système de vidéosurveillance fait l'objet de ce préavis pour autant que le champ de vision de ses caméras couvre tout ou partie de lieux publics (art. 2 al. 1 LVid). Au vu des informations fournies par le requérant, les caméras capturent des images des caisses (trois caméras) et de la zone mesures administratives-retrait de permis de conduire (deux caméras).

Le but du présent préavis est de vérifier la licéité de l'installation du système de vidéosurveillance dont il est question ici. Nous examinons d'abord l'analyse des risques (cf. chap. II), ensuite le respect des principes généraux et autres conditions légales, à savoir l'exigence de la base légale, le respect du

principe de la proportionnalité, le signalement adéquat du système, le respect du principe de la finalité, la sécurité des données et la durée de conservation des images (cf. chap. III, ch. 1 à 6).

Au terme de l'art. 2 LVid, « la présente loi s'applique aux installations de vidéosurveillance portant en tout ou en partie sur des lieux publics ». Sont également des lieux publics, les immeubles ouverts au public qui sont affectés à l'administration publique (cf. art. 2 al. 2 let. b LVid). Conformément à l'art. 1 al. 1 de la loi du 7 mai 1996 sur l'Office de la circulation et de la navigation (LOCN ; RSF 122.23.7) « l'Office de la circulation et de la navigation [...] est un établissement de droit public, doté de la personnalité juridique ». Par conséquent, les espaces dans les bâtiments de l'OCN mis à la disposition du public sont à considérer comme étant un lieu public au sens de la LVid.

II. Analyse des risques

1. Analyse préalable des risques et des mesures de prévention au regard du but poursuivi (art. 3 al. 2 let. e OVID)

Le but du présent système de vidéosurveillance est « de dissuader tout comportement violent ou autre mesure de contrainte vis-à-vis du personnel de l'OCN. Le cas échéant, il doit permettre l'identification d'éventuels agresseurs [...] » (cf. art. 1 ch. 3 du Règlement d'utilisation).

Une analyse complète des risques, à la lumière du principe de la proportionnalité, ne figure pas au dossier. En l'état, on peut déduire des éléments à notre disposition ce qui suit :

1.1 Quant à l'analyse des risques

Il s'agit de déterminer s'il peut y avoir des atteintes contre des personnes ou des biens dans les lieux à protéger ou s'il y a un danger concret que des atteintes se produisent. Si le dossier ne mentionne pas de cas d'atteintes contre des personnes ou des biens, il est cependant concevable que de telles atteintes puissent survenir à l'encontre des collaboratrices et collaborateurs de l'OCN, notamment sur le personnel travaillant aux caisses avec des liquidités (vol, brigandage etc.) ainsi que sur le personnel exerçant leur activité dans le secteur des mesures administratives, telles que les retraits de permis (contraintes, menaces etc.).

1.2 Quant aux moyens

Il s'agit de déterminer quels sont les moyens actuels et quels seraient les moyens possibles et moins radicaux que la vidéosurveillance. En l'espèce, pour protéger les collaborateurs de l'OCN, il semble que la vidéosurveillance soit un moyen efficace pour y parvenir. Si le nombre de caméras peut sembler important, leur champ de vision, somme toute restreint et axé sur les guichets, selon les informations à notre disposition, pour les trois caméras filmant les caisses et aux alentours du guichet, pour celles se trouvant dans la zone des mesures administratives, ne rend pas en l'état l'ensemble de l'installation disproportionnée.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est de « dissuader tout comportement violent ou autre mesure de contrainte vis-à-vis du personnel de l'OCN. Le cas échéant, il doit permettre l'identification d'éventuels agresseurs [...] ». Dès lors, il paraît envisageable que les moyens prônés permettent de remplir le but poursuivi et de limiter les risques cités plus haut.

III. Conditions

1. Exigence de la base légale

L'art. 38 Cst prévoit que « toute restriction d'un droit fondamental ou social doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi ». En l'occurrence, c'est le cas dans la LVid. En outre, conformément à l'art. 4 LPrD, le traitement de données personnelles ne peut se faire que si une disposition légale le prévoit, ce qui est le cas également.

2. Respect du principe de la proportionnalité (art. 4 al. 1 let. a LVid)

L'art. 4 LVid prévoit que les systèmes de vidéosurveillance avec enregistrement sont soumis au respect du principe de la proportionnalité (let. a).

Si la mesure paraît apte à atteindre le but visé, il n'en demeure pas moins que la surveillance doit être adéquate, c'est-à-dire apte à atteindre le but visé mais également limitée à ce qui nécessaire. En l'état, il apparaît que le choix est dicté par le fait qu'aucun autre système ne permette de remplir le but visé, tout en étant économiquement supportable (p. ex. substitution de la caméra par un vigile ou un système d'alarme).

3. Signalement adéquat du système (art. 4 al. 1 let. b LVid)

Conformément à ce qui est mentionné à l'art. 4 al. 1 let c LVid ainsi qu'à l'art. 8 OVID, tout système de vidéosurveillance devra être signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée et mentionnant le responsable du système, par exemple sous la forme de pictogrammes. Des documents à disposition, il ne ressort pas que l'information soit prévue.

4. Respect du principe de la finalité (art. 4 al. 1 let. c LVid)

Le principe de la finalité au sens de l'art. 5 LPrD est respecté dans la mesure où les données sont traitées conformément à l'art. 3 al. 1 LVid, à savoir de prévenir *les atteintes aux personnes et aux biens et de contribuer à la poursuite et à la répression des infractions*. Il apparaît, selon les informations à notre disposition, que le but visé par le requérant, est de *dissuader tout comportement violent ou autre mesure de contrainte vis-à-vis du personnel de l'OCN. Le cas échéant, il doit permettre l'identification d'éventuels agresseurs [...]*. Cette finalité paraît en adéquation avec l'exigence légale.

5. Sécurité des données (art. 4 al. 1 let. d LVid)

L'art. 5 du Règlement d'utilisation ne prévoit pas de mesures de sécurité en présence d'images à qualifier de sensible. Au terme de l'art. 3 let. c LPrD, sont des données sensibles, « les données personnelles sur : les opinions ou activités religieuses, philosophiques, politiques ou syndicales (ch. 1) ; la santé, la sphère intime ou l'appartenance à une race (ch. 2) ; des mesures d'aide sociale (ch. 3) ; des sanctions pénales ou administratives et les procédures y relatives (ch. 4) ». Or, notre Autorité a toujours considéré que le contexte pouvait rendre des données sensibles. Ainsi, le fait pour une personne d'être filmée en se rendant au guichet des mesures administratives peut constituer un traitement de données sensibles, parce que l'image est liée à des personnes clientes de l'OCN, dès lors que des personnes sont sous le coup d'une mesure administrative (sanction administrative). En effet,

c'est le contexte qui peut rendre les images obtenues sensibles, au sens de l'art. 3 let. c LPrD. Le ch. 3 du Règlement d'utilisation devra donc être modifié dans le sens de ce qui précède et prévoir des mesures de sécurité appropriées (comme p. ex. de sécuriser l'accès aux images au moyen d'un mot de passe ou d'installer un système de brouillage des images, etc.).

Par ailleurs, les données ne doivent être accessibles que par les personnes autorisées, comme cela est mentionné à l'art. 2 ch. 2 du Règlement d'utilisation. Finalement, le système doit être protégé dans un lieu adéquat et non-accessible à des personnes non-autorisées.

6. Durée de conservation des images (art. 4 al. 1 let. e LVID)

Conformément à l'art. 4 al. 1 let. e LVID, les images récoltées par une installation de vidéosurveillance doivent être conservées pendant *trente jours*, sauf en cas d'atteintes aux personnes ou aux biens auquel cas le délai peut être porté à cent jours (art. 4 ch. 3 du Règlement d'utilisation).

IV. Conclusion

L'Autorité cantonale de la transparence et de la protection des données émet un

préavis favorable à la demande d'autorisation d'un système de vidéosurveillance

par

l'Office de la circulation et de la navigation, route de Tavel 10, case postale 192, 1707 Fribourg, aux conditions suivantes :

- a. *signalément* : le système de vidéosurveillance devra être signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée et mentionnant le responsable du système, par exemple sous la forme de pictogramme.
- b. l'art. 5 ch. 3 du Règlement d'utilisation doit être modifié afin d'intégrer la possibilité d'enregistrer des données sensibles au sens de l'art. 3 let. c LPrD et de prévoir des mesures de sécurité appropriées (de sécuriser l'accès par un mot de passe, d'installer un système de brouillage des images, etc.) ; le système de stockage des données doit être protégé dans un lieu adéquat et non-accessible à des personnes non-autorisées.

V. Remarques

- > Les dispositions légales pertinentes doivent être respectées, notamment celles en matière de protection des données. Les données qui sont accessibles au service requérant ne doivent être consultées que dans le but pour lequel l'autorisation de l'installation de vidéosurveillance a été demandée. Les dispositions pénales sur le secret de fonction s'appliquent: les données consultées ne doivent pas être communiquées à d'autres organes publics ou à des personnes privées.
- > Toute modification de l'installation et/ou de son but devra être annoncée et notre Autorité se réserve le droit de modifier son préavis (art. 5 al. 3 OVID).
- > L'art. 30a al. 1 let. c LPrD est réservé.
- > Le requérant est rendu attentif que le champ d'application de la LVID ne couvre pas le fait de filmer ses employés-ées par les organes publics, ni l'utilisation des images récoltées à d'autres fins que celles pour lesquelles elles ont été enregistrées (art. 6 LPrD). Dans des cas d'espèce, certains comportements filmés peuvent toutefois entraîner l'application d'autres dispositions légales.



Dominique Nouveau Stoffel
Préposée cantonale à la protection des données

Annexes

- formulaire de demande d'autorisation d'installer un système de vidéosurveillance
- règlement d'utilisation