



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et
de la protection des données APrD
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. : RPA/FH – 2014-LV-13

PRÉAVIS du 16 septembre 2014

À l'attention du Préfet de la Broye, M. Christophe Chardonnens

Demande d'autorisation d'installation de vidéosurveillance sise à la Succursale de l'Office de la circulation et de la navigation, Route de l'Industrie 99, 1564 Domdidier,

p.a. 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 sis à la Succursale de l'OCN, Route de l'Industrie 99, 1564 Domdidier, comprenant deux caméras de marque Siemens, dôme avec zoom, montage apparent, liaison par câble, enregistrement sur serveur dédié, fonctionnant 24h/24 et activées par un détecteur de mouvement.

Ce préavis se base sur les éléments qui ressortent des formulaires de demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement datés du 21 mai 2014 et du 27 juin 2014 et de son Règlement d'utilisation (Annexe 1), transmis par la Préfecture de la Broye par courrier du 17 juillet 2014.

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). 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 la Succursale de l'OCN à Domdidier mis à la disposition du public sont à considérer comme étant un lieu public au sens de la LVID. Au vu des informations fournies par le requérant, deux caméras fixes capturent des images du rez-de-chaussée dont le sas d'entrée ainsi que le hall administration de la Succursale OCN de Domdidier. Cette dernière pouvant accueillir des personnes externes (automobilistes, clients, etc.) devient un lieu accessible au public, de sorte que le système de vidéosurveillance entre pleinement dans le champ d'application de la LVID.

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).

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 ses collaborateurs, l'OCN recourt aux guichets partiellement sécurisés ainsi qu'au paiement par cartes. Partant, la vidéosurveillance serait un moyen complémentaire et semble efficace pour les protéger. De plus, le nombre de caméras (2) ne paraît pas en l'état disproportionné.

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 le moyen prôné permette 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).

La vidéosurveillance porte atteinte à plusieurs libertés : la liberté personnelle, et plus particulièrement la triple garantie de l'intégrité physique et psychique et de la liberté de mouvement (art. 10 al. 2 Cst), le droit au respect de la sphère privée (art. 13 al. 1 Cst et 8 CEDH), le droit d'être protégé contre l'emploi abusif des données personnelles (art. 13 al. 2 Cst) et la liberté de réunion (art. 22 Cst ; cf. Alexandre Flückiger/Andreas Auer, La vidéosurveillance dans l'œil de la Constitution fédérale, AJP/PJA 2006, p. 931).

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 est 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. b 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 forme de pictogramme. 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. C'est le cas de prises de vue qui donneraient des informations par ex. sur la race, la sphère intime (accompagnants) et la santé (handicapés). 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 sont conservées pendant *trente jours*, sauf en cas d'atteintes aux personnes ou aux biens auquel cas le délai peut être porté à cent jours (cf. art. 4 ch. 3 du Règlement d'utilisation), ce qui est conforme avec la législation en vigueur.

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 à la Succursale de l'Office de la circulation et de la navigation, Route de l'Industrie 99, 1564 Domdidier

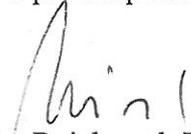
par

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

- a. *signalement* : 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 forme de pictogramme.
- b. *sécurité des données* : 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 (comme p. ex. 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 requérant ne doivent être consultées que dans le but pour lequel l'autorisation de l'installation de vidéosurveillance a été demandée. Les données consultées ne doivent pas être communiquées à des 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).
- > Le requérant est rendu attentif que le champ d'application de la LVID ne couvre pas le fait de filmer ses employés-ées, 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.
- > L'art. 30a al. 1 let. c LPrD est réservé.
- > Le présent préavis sera publié.


Alice Reichmuth Pfammatter
Préposée cantonale à la protection des données



Annexes

—

- formulaires de demande d'autorisation d'installer un système de vidéosurveillance
- Règlement d'utilisation
- dossier en retour