ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence, de la protection des données et de la médiation ATPrDM
Kantonale Behörde für Öffentlichkeit, Datenschutz und Mediation ÖDSMB

La Préposée cantonale à la protection des données *a.i.*

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08
www.fr.ch/atprdm
—
Réf. : MS/nk 2021-LV-24

PRÉAVIS
du 11 janvier 2023

À l'attention de la Préfète de la Sarine, Mme Lise-Marie Graden

Demande d'autorisation d'installation de vidéosurveillance avec enregistrement sise au Bâtiment scolaire communal, Route du Centre 10, 1741 Cottens
sise à la Déchetterie communale, route de Chavailles 27, 1741 Cottens

Commune de Cottens, Route du Centre 20, 1741 Cottens

I. Généralités

Vu

- les articles 12, 24 et 38 de la Constitution du canton de Fribourg du 16 mai 2004 (Cst ; RSF 10.1) ;
- l'article 5 alinéa 2 de la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance (LVid ; RSF 17.3) ;
- l'article 5 alinéa 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) ;
- la Loi cantonale du 4 avril 1972 sur le domaine public (LDP ; RSF 750.1),

l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM) formule le présent préavis concernant la requête de la commune de Cottens (ci-après : la requérante) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis au Bâtiment scolaire communal, Route du Centre 10, 1741 Cottens, et sis à la Déchetterie communale, route de Chavailles 27, 1741 Cottens, comprenant 4 caméras _____ avec un système de reconnaissance faciale et de véhicules et de comptage de personnes. Le système envisagé aux abords du bâtiment scolaire fonctionne en dehors des heures d'école.

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 12 avril 2022, de son Règlement d'utilisation ainsi que des annexes, transmis par la Préfecture de la Sarine par courrier du 26 avril 2022.

Le système de vidéosurveillance fait l'objet de ce préavis pour autant que le champ de vision de ses caméras couvre tout ou une partie de lieux publics (art. 2 al. 1 LVid). Sont des lieux publics, les

immeubles qui appartiennent au domaine public cantonal ou communal (cf. art. 2 al. 2 let. a LVid). Aux termes de l'article 3 alinéa 2 LDP, les routes communales, les places, les voies de communication et les biens communaux appartiennent au domaine public ainsi que les immeubles affectés à l'administration communale. Au vu des informations fournies par la requérante, les caméras capturent des images des abords de l'école communale, de la déchetterie communale et du local de l'édilité et du chauffage à distance (ci-après : CAD). Ainsi le présent 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. À cette fin, celui-ci donne « les détails techniques ou concrets » sur lesquels il se fonde (TC FR 602 2017 100 à 106 et 111 du 20 janvier 2020, consid. 5.2.). Ainsi il est d'abord examiné les risques (*cf.* chap. II), ensuite le respect des principes généraux et autres critères légaux, 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, la durée de conservation des images, l'information aux collaborateurs et collaboratrices, le droit d'accès, le respect de la confidentialité et l'obligation de déclarer les fichiers (*cf.* chap. III, ch. 1 à 10).

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 « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts au patrimoine communal » (*cf.* art. 1 ch. 3 du Règlement d'utilisation, ci-après : RU).

Une analyse des risques, à la lumière du principe de la proportionnalité, ne figure pas au dossier. Sur la base des éléments à notre disposition, il peut être déduit 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 s'y produisent. Il ressort du dossier que le terrain multisports a fait l'objet d'une réfection en 2021, par la suite de vandalisme. Les coûts de réfection s'élèvent à CHF 3'457.15. La requérante a également fourni des images de fenêtres brisées, de grillages endommagés et de tags. Le dossier ne mentionne, toutefois, pas dans quel intervalle ni dans quelle tranche horaire ont eu lieu ces actes (ni la ou les date(s) d'évènement). La requérante chiffre les dommages subis au local de l'édilité et à la déchetterie à CHF 15'000.

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. Il ne ressort pas du dossier que des mesures aient été mises en place ou éprouvées. Des lumières avec détecteur de mouvement sont des moyens qui permettent de décourager les actions dans l'obscurité, notamment après les heures de fermeture. Une sensibilisation des habitants de la commune doit être mise en place.

Des mesures moins attentatoires seraient des contrôles aléatoires effectués par le personnel, voire la présence de personnes sur place, etc.

1.3 Quant au but

Comme mentionné au point II. 1, le but du présent système est « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts au patrimoine communal » (*cf.* art. 1 ch. 3 RU).

Aux termes de l'article 3 alinéa 1 LVid, la vidéosurveillance veille à prévenir les atteintes aux personnes et aux biens et contribue à la poursuite et répression des infractions. Ces deux conditions, soit la prévention des atteintes aux biens et/ou aux personnes et la contribution à la poursuite et à la répression d'infractions, sont cumulatives (TC FR 601 2014 46 du 20 août 2015, consid. 3d)).

Le but susmentionné semble entrer dans le champ d'application de la LVid. Ainsi il paraît envisageable que le moyen projeté permette de remplir les buts poursuivis.

III. Conditions

1. Exigence de la base légale

L'article 38 Cst./FR déclare 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 ». Selon l'article 4 LPrD, le traitement de données personnelles ne peut se faire que si une disposition légale le prévoit.

Ainsi les traitements de données personnelles qu'implique la vidéosurveillance ainsi que les éventuelles restrictions qu'elle engendre sont régis par la LVid.

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

L'article 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 (not. art. 11 al. 2 Cst./FR ; art. 12 al. 1 Cst./FR et art. 8 CEDH ; art. 12 al. 2 Cst./FR : cf. FLÜCKIGER/AUER, La vidéosurveillance dans l'œil de la Constitution fédérale, AJP/PJA 2006, p. 931).

La surveillance doit être adéquate ; c'est-à-dire apte à atteindre le but visé et limitée à ce qui est nécessaire. La surveillance au moyen d'enregistrements vidéo permet la constatation d'infractions en assurant la conservation des preuves et en permettant ainsi un taux d'élucidation élevé. Grâce à l'effet dissuasif qui y est lié, les infractions sont combattues dans un but de maintien de la sécurité et de l'ordre public (TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire (FLÜCKIGER/AUER, op. cit., p. 938). Concrètement, la vidéosurveillance doit se limiter aux endroits où, selon l'expérience, se déroulent plus fréquemment des actes de vandalisme et dans lesquels règne par conséquent un plus grand sentiment d'insécurité. Le principe de la proportionnalité s'oppose à une vidéosurveillance généralisée de tout le territoire sans tenir compte du niveau d'insécurité qui y règne (FLÜCKIGER/AUER, op. cit., p. 938). En l'espèce, l'installation des caméras aux abords de l'école communale, de la déchetterie communale et du local de l'édilité et CAD est apte à limiter les atteintes aux biens et peut comporter un effet dissuasif.

Le principe de la proportionnalité ne s'applique pas seulement à la surveillance elle-même, mais également au dispositif technique choisi (Message n° 202 du Conseil d'Etat du 6 juillet 2010 accompagnant le projet de loi sur la vidéosurveillance, *in* BGC novembre 2010 1967, p. 1969).

L'atteinte est grave si la vidéosurveillance est doublée d'un traitement informatisé permettant de suivre automatiquement une scène, d'initier des alarmes en fonction de l'analyse de comportement types ou de caractéristiques prédéfinis. Le recours à Internet pour le transit des données, leur visualisation ou le pilotage des caméras augmente l'atteinte potentielle, en particulier en l'absence d'un système de cryptage permettant aisément de diffuser ces données sans restriction (FLÜCKIGER/AUER, op. cit., p. 934). Selon les informations communiquées, la transmission est réalisée par câbles. L'enregistrement ainsi que la vision en direct sont envisagés. Or, pour que le présent système soit conforme au principe de la proportionnalité, une vidéosurveillance avec enregistrement simple, dont l'enregistrement est effacé automatiquement après une brève durée qui n'est pas doublé d'un suivi en temps réel et est visionné et utilisé uniquement en cas de délits avérés, est largement suffisante pour les caméras sur le domaine public (place et lieux de passage). Selon la jurisprudence et les recommandations du Préposé fédéral à la protection des données et à la transparence[1], le dispositif technique utilisé doit également respecter le principe de proportionnalité, notamment en préservant l'anonymat des personnes. En l'occurrence, un système de floutage des images ou des bandes noires doit être employé afin de réduire au maximum l'atteinte aux libertés des personnes filmées, de sorte que l'installation ne doit filmer que les parties absolument nécessaires. En cas d'infractions avérées, les floutages peuvent être ponctuellement désactivés afin de dévoiler l'identité du responsable (cf. Arrêt TC FR 601 2014 46, consid. 3b). L'efficacité des systèmes de vidéosurveillance n'est ainsi aucunement réduite.

Sous l'angle de la nécessité, la vidéosurveillance ne constitue en l'espèce pas le seul moyen propre à atteindre les buts visés, mais d'autres mesures moins restrictives par rapport aux libertés en cause permettent d'arriver aux mêmes fins (un éclairage par détection de mouvement aux lieux sensibles, une sensibilisation active des habitant-e-s, des contrôles aléatoires effectués par le personnel, etc., *cf.* chap. 2, ch. 1.2).

Sous l'angle du principe de la proportionnalité au sens étroit, l'intérêt public à la prévention et à la répression d'infractions (dégâts matériels, atteintes à la personne) doit primer l'intérêt privé au respect des libertés personnelles des personnes (TC FR 601 2014 46, consid. 2b/cc et réf. citées). L'intérêt public à installer des caméras afin de lutter contre des vols et/ou déprédations ne l'emporte pas sur l'intérêt des personnes à protéger leur personnalité. Pour que l'atteinte aux libertés ne soit pas disproportionnée, il est indispensable de veiller, au besoin par des moyens techniques de blocage, à ce que les caméras vidéo ne puissent pas être dirigées contre des immeubles ou des maisons privées sis à proximité des lieux sensibles où le regard indiscret ou distrait de l'observateur risquerait de porter une atteinte en tout point inadmissible à la sphère privée ou au domaine secret des habitants (*cf.* FLÜCKIGER/AUER, op. cit., p. 940). Ainsi un système de masquage de zone (cache ou bloque noir) doit être employé en présence d'habitations privées dans le champ de vision. Il sied de rappeler que les installations situées dans des lieux de passages fréquents portent de plus grandes atteintes aux libertés des personnes qu'une surveillance dans un endroit à l'écart (TC FR 601 2014 46, consid. 3b) cc et réf.). Les sites concernés sont proches de routes et d'habitations. Il s'agit ainsi de lieux de passage (voire proches de passages).

---

[1] https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-dans-les-vestiaires-et-dan.html).

Afin d'avoir une vue générale, chaque caméra est analysée à la lumière du principe de la proportionnalité, sous réserve des champs de vision définitifs. Il est relevé que l'appréciation est réalisée d'après les plans transmis ; c'est-à-dire les images figurant au dossier. Afin de simplifier la lecture, nous abordons les caméras dans l'ordre croissant :

- **Bâtiment scolaire communal :**

  > **Caméras 1 et 2 – enregistrement des images et vision en temps réel.** Se pose la question de la nécessité d'avoir deux caméras. Une caméra au centre du terrain bénéficierait d'un angle de vue couvrant l'entier du terrain. Une caméra est favorisée et le champ de vision est adapté en conséquence. Le RU est modifié en ce sens. La vision en temps réel n'est pas proportionnée (cf. ci-dessous) ;

  > **Caméra 3 – enregistrement des images et vision en temps réel.** La question de la nécessité de la caméra se pose, au vu de la présence de l'autre caméra. La vision en temps réel n'est pas proportionnée (cf. ci-dessous) ;

- **Déchetterie communale :**

  > **Caméra 1 – enregistrement des images et vision en temps réel.** La volonté est de prévenir les atteintes aux bâtiments ainsi qu'au matériel (not. véhicule). Des images des dommages sont fournis par la requérante. À défaut de champ de vision des angles de vue des caméras, la proportionnalité ne peut être arrêtée de manière définitive. Les champs de vision définitifs sont communiqués à la Préfecture pour analyse. La vision en temps réel n'est pas proportionnée (cf. ci-dessous).

Aux termes de l'article 1 chiffre 5 RU, le système fonctionne en dehors des heures d'école pour les caméras aux abords du bâtiment scolaire. Toutefois, l'horaire de fonctionnement fait défaut concernant la zone déchets verts, le local d'édilité et le CAD. Il importe de relever que la requérante n'a pas précisé quand (tranches horaires) les dommages ont eu lieu. Sur la base du dossier, il peut être admis que la présence du personnel sur place est généralement un moyen efficace de dissuasion. Un horaire en dehors des heures de présence du personnel est à favoriser. Le RU est modifié en ce sens.

Il sied de rappeler que l'atteinte est plus grave lorsque l'enregistrement est doublé de la vision en direct (cf. ci-dessus) ; d'autant plus lors qu'il s'agit de mineurs en scolarité obligatoire. En outre, en dehors des heures scolaires ou d'ouverture de la déchetterie, il ne semble pas que la présence d'un concierge, d'un vigile ou d'un membre du personnel soit prévue. Dans cette compréhension, la vision en temps réel ne passe pas l'examen de la proportionnalité. En effet, le but de surveillance peut être atteint par l'enregistrement.

Conformément au principe de la proportionnalité, l'enregistrement des images doit être enclenché à la suite de la détection de mouvement. Le RU est précisé en ce sens. La reconnaissance faciale ou de véhicule(s) n'est pas autorisée ni le système de comptage de personnes. Il s'agit d'un système d'intelligence artificielle portant une atteinte grave à la personnalité. En outre, la reconnaissance faciale ou de véhicule(s) nécessite une base légale pour permettre une interconnexion avec d'autres bases de données (TF, 1C_39/2021 du 29 novembre 2022, consid. 8.5 et réf. citées). Le RU est modifié en ce sens.

En cas d'atteinte, l'image est « extraite » en attente de la demande de l'Autorité compétente (enregistrement sur support à part). L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale ou de véhicule(s), n'est pas autorisée.

Enfin, afin que ce système de surveillance soit toujours conforme aux besoins et aux conditions légales, une réévaluation peut être opérée dans un délai de trois ans concernant notamment les risques d'atteinte et la portée de la mesure.

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

Le système doit être signalé à ses abords de manière adéquate (art. 4 al. 1 let. b LVid). Partant, le RU est complété de la manière suivante : « le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée (p. ex. sous la forme d'un pictogramme) et mentionnant le responsable du système ».

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

La finalité paraît en adéquation avec l'exigence légale (art. 1 ch. 3 RU).

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

Le Conseil communal est l'organe responsable du système de vidéosurveillance conformément à l'article 2 alinéa 1 lettre c OVid. Nous conseillons de modifier l'article 2 chiffre 1 RU en ce sens.

Pour tout accès direct aux images de la part de la police cantonale, une base légale est nécessaire. Les agents et agentes de la police cantonale peuvent examiner les moyens de preuve conformément aux codes de procédures idoines. Concernant l'activité policière et les mesures d'élucidation de l'infraction, le Code de procédure pénal s'applique (TF, 1C_39/2021 du 29 novembre 2022, consid. 4.1.2). Partant, le RU est modifié concernant l'accès par les agents et agentes de la police cantonale.

Il importe de distinguer les différentes autorisations ainsi que les droits d'accès y relatifs selon les fonctions et les rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, etc.). Les titulaires d'autorisation personnelle (art. 2, ch. 2, RU) consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée. La double authentification pour l'accès est conseillée.

En cas d'atteinte, l'image est « extraite » en attente de la demande du juge (enregistrement sur support à part). L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale ou de véhicule(s) ou un système de comptage de personnes, n'est pas autorisée.

Concernant la sécurité des données, les informations relatives au fournisseur ou à l'entreprise d'installation et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) doivent faire l'objet d'une analyse spécifique. Le contrôle

interne du système doit avoir lieu sur le site. En cas de sous-traitance, les articles 18 et 12*b* ss LPrD doivent être respectés.

Nous conseillons de prévoir une information dans le RU quant à la limitation de l'accès au serveur local ainsi qu'au local où sont stockés les enregistrements et/ou extractions aux seules personnes autorisées (*cf.* art. 2, ch. 2, RU). Le lieu d'hébergement des données, la localisation du serveur local ainsi que des précisions quant au réseau utilisé sont renseignés à la Préfecture.

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

A moins qu'elles ne soient conservées dans le cadre d'une procédure, les données enregistrées doivent être détruites après 30 jours ou, en cas d'atteinte aux personnes ou aux biens, après 100 jours au maximum. Dans tous les cas, nous conseillons d'effectuer une analyse pour déterminer si les données peuvent être détruites après un délai plus court que les 30 jours prévus par la loi. En raison de la jurisprudence du Tribunal fédéral (cf. ATF 133 I 77, JdT 2007 I 591) et des recommandations du Préposé fédéral à la protection des données et à la transparence[2], notre Autorité conseille une destruction automatique après 10 jours. Les infractions contre les biens étant constatées par les autorités étatiques elle-même (et non sur plainte) une longue durée de conservation ne nous semble pas indispensable en cas d'atteinte.

En cas d'atteinte avérée aux personnes ou aux biens, les données enregistrées sont extraites sur un support informatique et sont détruites après 100 jours au maximum. Un protocole de destruction est conservé. Les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Le RU devrait préciser ces aspects.

7. Informations aux collaboratrices et collaborateurs

La requérante est rendue attentive au fait que, dans la mesure où elle filme ses employé-e-s, ces derniers doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

8. Droit d'accès (art. 1 al. 2 in fine LVid ; art. 23 LPrD)

Un article relatif au droit d'accès devrait être ajouté dans le RU. Celui-ci précise ainsi que « toute personne peut demander au responsable du système l'accès à ses propres données. Le responsable du système répond à la demande tout en respectant les droits de la personnalité des autres personnes concernées (en les floutant par exemple) ».

9. Clause de confidentialité

Le prestataire mandaté ainsi que ses collaboratrices et collaborateurs doivent signer une clause de confidentialité, réservant des suites juridiques en cas de non-respect, dans la mesure où il s'agit de données sensibles et soumises au secret de fonction.

En effet, quand bien même le secret de fonction s'applique aux fonctionnaires, la notion d'auxiliaire, qui comprend non seulement la personne effectivement apte à remplir la mission confiée et qui

---

[2] (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html)

l'accepte ainsi que toutes celles qui participent effectivement à l'accomplissement de la tâche liée à l'exécution du mandat ou du contrat, s'applique par analogie à l'article 320 du Code pénal suisse (concernant le secret de fonction). Le secret de fonction[3] étant applicable à l'auxiliaire, le contrat de service ou de mandat se doit de préciser cela (*cf.* MÉTILLE, L'utilisation de l'informatique en nuage par l'administration publique, AJP/PJA 6/2019, p. 609 ss, p. 613 s.). Nous conseillons de prévoir que la clause de confidentialité soit annexée au RU (art. 7 RU).

10. Déclaration de fichier

Conformément aux articles 19 ss LPrD, les fichiers doivent être déclarés à l'ATPrDM avant leur ouverture

[3] À ce sujet, voir également : (*cf.* BO CN 22.7249 Keller-Sutter Karin, L'usage d'un service de cloud à l'étranger par une entité soumise à l'art. 320 CP constitue-t-elle une violation du secret de fonction ?).

IV. Conclusion

Dans le cadre de la demande d'installation du système de vidéosurveillance avec enregistrement sis au **Bâtiment scolaire communal**, Route du Centre 10, 1741 Cottens, et sis à la **Déchetterie communale**, route de Chavailles 27, 1741 Cottens

par

la commune de Cottens, Route du Centre 20, 1741 Cottens

l'Autorité cantonale de la transparence, de la protection des données et de la médiation émet un :

- **partiellement favorable** à la demande d'installation, avec enregistrement, des **caméras.** En effet, nous préavisons défavorablement la vision en temps réel ;

aux conditions suivantes :

a. analyse des risques : l'organe responsable peut réévaluer le système de vidéosurveillance, la situation, les risques et les moyens dans un délai de trois ans.

b. proportionnalité : Des informations complémentaires sont fournies à la Préfecture concernant le besoin et la nécessité d'installer les trois caméras (caméras 1, 2 et 3 au bâtiment scolaire, cf. ci-dessus) pour une appréciation définitive. L'angle de vision de la caméra envisagée dans la zone verte de la déchetterie est communiqué à la Préfecture pour appréciation définitive. Le nombre de caméra est adapté et figure dans le RU. Le RU est modifié en ce sens.

Concernant l'horaire de fonctionnement des caméras, un horaire en dehors des heures d'ouverture du site et des heures scolaires est favorisé. Le RU est précisé en ce sens, notamment concernant la déchetterie. Pour la déchetterie, le champ de vision définitif est communiqué à la Préfecture pour analyse. Les mécanismes de reconnaissance facile ou de véhicule(s) ainsi que tout système de comptage de personne ne sont pas autorisés. Le RU est précisé en ce sens.

La surveillance en extérieur nécessite la présence d'un système de masquage de zone (cache ou bloque noir) en présence d'habitations privées ou véhicules (plaque d'immatriculation) dans le champ de vision.

c. sécurité des données : L'article 2 chiffre 1 RU précise que le responsable du système est le Conseil communal.

Le RU est modifié concernant l'accès par les agents et agentes de la police cantonale (cf. ci-dessus). Les accès aux images et enregistrements et autorisations sont distinguées selon les fonctions et les rôles des personnes. Le RU est modifié en ce sens.

Les différentes autorisations ainsi que les droits d'accès y relatifs sont distingués selon les fonctions et les rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, etc.). Le RU précise que les titulaires d'autorisation consultent les images qu'en cas d'atteinte avérée. L'enregistrement des images fonctionne sur détection de mouvement. Les utilisateurs changent régulièrement leurs mots de passe. Une double authentification est conseillée.

L'article 4 RU est complété d'un chiffre distinguant les enregistrements continus standard des enregistrements faisant suite à une extraction de données ; d'un chiffre expliquant que les images sont uniquement enregistrées ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons, voire permettant la reconnaissance faciale ou de véhicule(s) ou un système de comptable de personne, n'est pas autorisée. Les images enregistrées et celles extraites sont stockées sur un support physique indépendant.

Les informations relatives au fournisseur ou à l'entreprise d'installation et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) font l'objet d'une analyse spécifique. Le contrôle interne du système doit avoir lieu sur le site. En cas de sous-traitance, les articles 18 et 12*b* ss LPrD doivent être respectés.

La limitation de l'accès au serveur local ainsi qu'au local où sont stockés les enregistrements et/ou extractions aux seules personnes autorisées (cf. art. 2, ch. 2, RU) est spécifiée dans le RU. La Préfecture est renseignée à ce sujet ainsi qu'en ce qui concerne la localisation du serveur local, le lieu d'hébergement des données et le réseau utilisé.

d. *signalement* : un chiffre est ajouté à l'article 1 RU avec la formulation suivante : « le système de vidéosurveillance est signalé à ses abords au moyen de panneaux informant sans équivoque les personnes se trouvant dans la zone surveillée (p. ex. sous la forme d'un pictogramme) et mentionnant le responsable du système ».

e. *destruction des images* : l'article 4 chiffre 3 RU doit déclarer qu'il incombe aux responsables de s'informer régulièrement de la situation.

Comme le mentionne le RU, les données enregistrées doivent être détruites automatiquement au maximum après 30 jours. L'examen d'une éventuelle destruction automatique après 10 jours est réalisé. En cas d'atteintes avérées aux personnes et aux biens, les enregistrements (extraction) peuvent être conservées jusqu'à 100 jours.

f. *informations aux collaboratrices et collaborateurs :* les collaboratrices et collaborateurs doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

g. *droit d'accès :* le RU est complété d'un article relatif au droit d'accès de toute personne souhaitant consulter ses propres données.

h. *clause de confidentialité :* le prestataire mandaté ainsi que ses collaboratrices et collaborateurs signent une clause de confidentialité.

i. *obligation de déclarer le fichier* : les fichiers doivent être déclarés à l'ATPrDM avant leur ouverture, conformément aux articles 19 ss LPrD.

V. Remarques

> Les dispositions légales pertinentes doivent être respectées, notamment celles en matière de protection des données. Les données qui sont accessibles à la requérante 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 l'Autorité se réserve le droit de modifier son préavis (art. 5 al. 3 OVid).

> L'article 30*a* alinéa 1 lettre c LPrD est réservé.

> Le présent préavis peut être publié.

Martine Stoffel
Préposée cantonale à la transparence
Préposée cantonale à la protection des données *a.i.*

Annexes
—
- Formulaire de demande d'autorisation d'installer un système de vidéosurveillance avec enregistrement
- Dossier en retour