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 à la transparence
La préposée 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-31

PRÉAVIS
du 20 octobre 2022

À l'attention du Préfet de la Gruyère, M. Vincent Bosson

Demande d'autorisation d'installation d'un système de vidéosurveillance avec enregistrement

Collège du Sud, Rue de Dardens 79, 1630 Bulle

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 11 avril 1991 sur l'enseignement secondaire supérieur (LESS ; RSF 412.0.1) ;
- le Règlement du 27 juin 1995 sur l'enseignement secondaire supérieur (RESS ; RSF 412.0.11),

l'Autorité cantonale de la transparence, de la protection des données et de la médiation (ATPrDM) formule le présent préavis concernant la requête du Collège du Sud (ci-après : CSUD ou requérant) visant à l'installation d'un système de vidéosurveillance avec enregistrement, sis au CSUD, Rue de Dardens 79, 1630 Bulle, comprenant 9 caméras de type _____, fonctionnant en semaine, de 19h00 à 7h00, et les week-ends et les vacances scolaires, 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, le Règlement d'utilisation et les annexes, transmis par la Préfecture de la Gruyère par courrier du 29 novembre 2021 ainsi que les compléments transmis par la Préfecture de la Gruyère par courriel du 12 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). Les

immeubles affectés à l'administration public appartiennent au domaine public cantonal (art. 2 al. 1 LESS ; art. 3 al. 1 ch. 1 LDP). Les routes, voies de communication et les places communales appartiennent également au domaine public (art. 3 al. 2 ch. 2 LDP). Au vu des informations fournies par le requérant, les caméras capturent des images de l'intérieur et de l'extérieur du bâtiment du CSUD, en particulier les entrées, cours et espaces et les chemins d'accès. 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 personnes sous vidéosurveillance, 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 « d'éviter les dégradations et le littering sur le terrain entourant le Collège du Sud » (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 biens dans les lieux à protéger ou s'il y a un danger concret que des atteintes se produisent. Le dossier mentionne des dommages sur l'extérieur des bâtiments et à l'extérieur des bâtiments, sur des panneaux d'interdiction, sur le poteau du parking, sur les tables extérieures (tags, début de feu, etc.) ainsi que des incivilités (mégots de cigarette, bouteilles en verre et déchets sauvages).

Le complément du courrier du 12 avril 2022 est accompagné d'un dossier photos « liste des dégâts » regroupant l'ensemble des dépravations et dégâts enregistrés sur le site du requérant. Il ressort du dossier que le montant des dommages est d'environ CHF 13'000.00. Il s'agit essentiellement d'estimations en raison des heures de travail effectuées par le service des bâtiments. Aucune plainte pénale n'a été portée à la connaissance de l'Autorité.

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.

Des mesures sont envisageables : la mise en place d'une surveillance, notamment par le concierge, voire des personnes habilitées, la fermeture à clé des bâtiments après les heures de cours, une sensibilisation des étudiants et des parents, etc. Le requérant n'apporte aucune précision quant aux raisons propres à

l'installation de la vidéosurveillance plutôt qu'à d'autres mesures, ni quels autres moyens ont été éprouvés et leurs résultats.

1.3 Quant au but

Comme mentionné au point II. 1.1, le but du présent système de vidéosurveillance est « d'éviter les dégradations et le littering sur le terrain entourant le Collège du Sud » (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)). Lorsque l'installation ne vise que la prévention et la répression d'infraction contre des biens, l'intérêt public a un poids plus faible (TC FR 601 2014 46 du 20.08.2015, consid. 3b) réf. citées).

Éviter les déprédations sur le patrimoine scolaire semble entrer dans le champ d'application de la LVid. La lutte contre les incivilités (mégots de cigarette, déchets sauvages, etc.) ou l'utilisation non conforme du matériel ou des locaux ne remplit pas les conditions de l'article 3 alinéa 1 LVid et ne saurait être observé au moyen de la vidéosurveillance, sans que l'on puisse constater une disproportion excessive entre le but poursuivi et le système de vidéosurveillance projeté (TC FR 601 2014 46 du 20 août 2015, consid. 3a). Partant, la formulation suivante est recommandée : « lutter contre les actes de déprédations sur les bâtiments et dans l'enceinte du Collège du Sud et contribuer à la poursuite et à la répression d'infractions ». 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 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'article 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'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 : la liberté personnelle, et plus particulièrement la triple garantie de l'intégrité physique et psychique et de la liberté de mouvement (art. 11 al. 2 Cst), le droit au respect de la sphère privée (art. 12 al. 1 Cst et 8 CEDH), le droit d'être protégé contre l'emploi abusif de ses données personnelles (art. 12 al. 2 Cst) et la liberté de réunion (art. 24 Cst ; *cf.* FLÜCKIGER/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. 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 publics (TC FR 601 2014 46 du 20 août 2015, consid. 2b/cc). En l'état, on peut dès lors admettre que l'installation

des caméras dans l'enceinte du bâtiment scolaire du Collège du Sud est apte à limiter les atteintes aux biens et peut comporter un effet dissuasif. Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire, c'est-à-dire dans les lieux où l'intérêt public visé ne parvient pas à être atteint par d'autres moyens (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).

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, seul l'enregistrement est envisagé. La 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 ainsi qu'utilisé uniquement en cas de délits avérés, est largement suffisante dans le cas d'espèce. 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. 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 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 floutage des images ou de bandes noires devrait être employé afin de réduire au maximum l'atteinte aux libertés des personnes filmées (l'installation ne doit filmer que les parties absolument nécessaires ; notamment en présence d'habitations privées dans le champ de vision, dans la mesure où l'école se trouve entourée d'habitations privées) (*cf.* commentaires ci-dessous par caméra). En cas d'infraction(s) avérée(s), le système de floutage ou la bande noire peut être ponctuellement désactivé afin de dévoiler l'identité du responsable (Arrêt TC FR 601 2014 46, consid. 3b). L'efficacité du système de vidéosurveillance n'est ainsi aucunement réduite. En outre, l'enregistrement ne peut être éventuellement admis que sous un horaire restreint, proportionné aux atteintes pour autant que le champ de vision soit adapté à ce qui est nécessaire.

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. En effet, une surveillance régulière, ou aléatoire, par une personne responsable permettrait également de limiter les atteintes aux biens et aux personnes (*cf.* chap. II, ch. 1.2). Filmer les entrées depuis l'extérieur des bâtiments est apte à atteindre le but. La surveillance à l'intérieur des bâtiments nécessite une base légale expresse au vu de la gravité de l'atteinte portée ;

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

notamment en raison de l'âge des élèves (mineurs). En effet, lorsque le « traitement de données personnelles peut constituer et constitue le plus souvent une limitation aux droits fondamentaux et à la liberté personnelle en particulier, cette limitation doit être prévue dans une disposition légale. […] La base légale doit être suffisamment précise pour que le citoyen puisse adapter son comportement et mesurer la conséquence d'un tel comportement avec une certaine certitude. […] Cela exclut en particulier la collecte de données « en prévision de… ». [….] Le degré de précision dépend du cercle des personnes concernées […]. Les limites imposées aux droits fondamentaux doivent être claires et reconnaissables pour l'individu » (*cf.* WALTER Jean-Philippe, Le droit public matériel, in Nicolas Gillard (édit.), La nouvelle loi fédérale sur la protection des données, Lausanne 1994, p. 41 ss, p. 59 ss).

Au sens 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 à lutter contre des déprédations ne l'emporte pas sur l'atteinte importante au droit de la personnalité des personnes concernées (*cf.* ci-dessus, atteinte grave à la 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.

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 sur la base des plans (avec rayons de visionnage) fournis au dossier ; c'est-à-dire en l'absence de champs de vision définitifs :

- **Cameras 1, 2, 3 – caméras intérieures. Enregistrement des images. Il n'y a pas de vision en temps réel.**

  Pour être proportionnée, la vidéosurveillance ne peut être installée qu'aux endroits où elle s'avère nécessaire, c'est-à-dire dans les lieux où l'intérêt public visé ne parvient pas à être atteint par d'autres moyens (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, il ressort du dossier que les dommages subis (chiffrés et estimés) concernent des actes perpétrés sur l'extérieur du bâtiment et dans l'enceinte de celui-ci. Selon les plans, l'entrée extérieure est filmée par d'autres caméras. Le requérant n'explique pas en quoi filmer l'intérieur est nécessaire. Une telle surveillance nécessite une base légale (*cf.* ci-dessus). Les caméras (caméra intérieure du rez, entrée depuis le sous-sol direction CO / camera intérieure du rez supp., entrée principale direction EPAC / camera intérieure du rez supp., entrée principale direction CO) ne respectent pas le principe de la proportionnalité.

- **Caméras 4, 5, 6 – extérieur en direction du terrain entre le collège et la salle Omnisport**. **Il n'y a pas de vision en temps réel.**

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). Les informations quant au lieu filmé (not. ce que le requérant souhaite filmer et protéger), les atteintes subies à ce lieu ainsi que la nécessité d'installer les caméras à ces endroits faisant défaut, il se pose la question de la proportionnalité au vu du nombre de caméras et de l'absence de champ de vision. Concernant l'arrière-fond n'entrant pas dans le but de la vidéosurveillance, un cache de confidentialité est envisagé par caméra. 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.).

Selon le document « liste des dégâts », des dommages ont été réalisés. Ce nonobstant, du dossier il ne ressort pas suffisamment clairement quelle caméra est concernée par quel dommage. Les informations étant lacunaire, la proportionnalité ne peut être admise de manière définitive.

Les informations ainsi que les images (champ de vision) sont transmises à la Préfecture pour analyse.

- **Caméras 7 et 8 – extérieur en direction du terrain entre le collège et les immeubles d'habitation. Il n'y a pas de vision en temps réel.**

  Il est renvoyé à l'argumentation des caméras 4, 5 et 6.

- **Camera 9 – extérieur du côté du cycle d'orientation – enregistrement des images. Il n'y a pas de vision en temps réel**.

  Il est renvoyé à l'argumentation des caméras 4, 5 et 6.

Le RU fait état de 6 caméras, alors qu'il ressort des documents communiqués que 9 caméras sont envisagées. Le RU est modifié dans ce sens (sous réserve des caméras autorisées par la Préfecture).

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.

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, 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)

Aux termes de la législation, le système doit être signalé à ses abords de manière adéquate (art. 4 al. 1 let. b LVid). Des documents à disposition, il ne ressort pas que l'information est prévue. Partant, le RU

est complété, par exemple à l'article 1, 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. 4 ch. 1 RU), sous réserve du chap. II, ch. 1.3.

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

Des informations complémentaires doivent être fournies concernant le cache confidentiel utilisé pour veiller aux intérêts de tiers (s'agit-il d'un cache fixe, amovible, pour qui et par qui ?).

L'organe responsable du système de vidéosurveillance est l'organe dirigeant (art. 2 al. 1 let. b OVid), c'est-à-dire la Direction du CSUD. Le RU est modifié en ce sens.

L'article 2 chiffre 2 RU parle de « flux direct ». Dès lors que seul l'enregistrement est envisagé, le RU doit être modifié. La terminologie peut être sujette à interprétation. Les titulaires d'autorisation personnelle (art. 2, al. 1, RU) consultent les images enregistrées qu'en cas de nécessité, à savoir en cas d'atteinte avérée. L'autorisation ainsi que les droits d'accès y relatifs doivent être distingués selon les fonctions et rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, etc.). En outre, il est rappelé que l'accès aux enregistrements est autorisé uniquement en cas d'atteinte avérée. Les utilisateurs devraient changer régulièrement le mot de passe. Ainsi une double authentification est recommandée. Il est recommandé, lorsqu'un (autre) article du RU cite les personnes autorisées d'insérer un lien, vers l'article 2 chiffre 2 RU.

Des précisions doivent être fournies concernant le serveur local. Une information est faite 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). L'hébergement des données est local, sans accès à distance. Le réseau utilisé est distinct de celui de l'école. Le RU est précisé en ce sens.

Concernant la sécurité des données, les informations relatives au fournisseur ou à l'entreprise d'installation et/ou de maintenance (si externalisation) et les mesures techniques (tels que le chiffrement du transfert et du stockage des données, le détenteur des clés, le contrat y relatif) font défaut et devront faire l'objet d'une analyse spécifique. En cas de sous-traitance, les articles 18 et 12*b* ss LPrD doivent être respectés. En effet, lorsque l'organe public fait traiter des données par une entreprise externe, des conditions plus strictes doivent être appliquées et doivent être réglées dans un contrat (art. 18 LPrD). Le contrat doit notamment contenir une garantie du niveau adéquat de protection des données ; le lieu du traitement des enregistrements doit être connu et sécurisé ; la durée du contrat ainsi que la durée de conservation des enregistrements doit être fixée ; les modalités de transfert des données du mandataire au requérant doivent être mises en place ; les responsabilités entre le mandataire et le sous-traitant doivent être réparties ; les modalités selon lesquelles les enregistrements sont sauvegardés, archivés et détruits doivent être décrites avec précision ; des contrôles doivent pourvoir être effectués par la requérante, la Préfecture ainsi que par l'ATPrDM, sur les activités du mandataire sous-traitant ; le for de la poursuite ainsi que le droit applicable sont suisses. En outre, les enregistrements doivent être chiffrés au niveau de la transmission et du stockage. La clé de cryptage doit être uniquement détenu par l'organe public, respectivement une des personnes autorisées à l'article 2 chiffre 2 RU. Le RU (art. 5 ch. 3 let. a RU) est modifié en ce sens. Le mandataire ne doit pas pouvoir avoir accès aux données. De

plus, la maintenance ne pourra pas être effectuée à distance. Les systèmes d'information utilisés (notamment _____) doivent respecter la LPrD et le RSD.

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

Concernant la durée de conservation, le Préposé fédéral à la protection des données et à la transparence (ci-après : PFPDT) recommande une durée de conservation de 24 à 72 heures[2]. Le Conseil d'État explique dans son Message relatif à la vidéosurveillance qu'« en ce qui concerne le délai de destruction des images enregistrées, […] le projet (let. e) propose un délai qui est suffisant pour que la personne qui visionne les images soit en mesure de réagir (information donnée à son supérieur ; dénonciation pénale, …). Sous cet angle, un délai maximal de 7 jours semble adéquat. […] Un tel délai, jugé admissible par le Tribunal fédéral, est suffisant pour que la collectivité puisse réagir et prendre le cas échéant la décision de dénoncer pénalement les comportements visionnés » (*cf.* Message n° 202, op. cit., p. 1969). En effet, comme la vidéosurveillance est souhaité pour « la prévention des actes de vandalisme et l'identification des personnes ayant causé des dégâts au patrimoine communal », la conservation des images devrait être restreinte. Dans cet ordre d'idées, le Tribunal fédéral rappelle qu'il faut distinguer entre les infractions commises contre des biens et celles commises contre des personnes. Les infractions contre les biens étant constatées par les autorités étatiques elle-même (et non sur plainte) une longue durée de conservation n'est pas indispensable en cas d'atteinte (*cf.* ATF 133 I 77, JdT 2007 I 591). Ainsi le délai légal est un maximum qui doit être apprécié à la lumière du cas d'espèce. Par ailleurs, les responsables doivent s'informer régulièrement de toute situation pouvant entrer dans le but de la protection. Partant, les données doivent être détruites après 10 jours (automatiquement). En cas d'atteintes avérées aux personnes ou aux biens, les enregistrements peuvent être extraits et conservés jusqu'à 100 jours, de manière sécurisée. Le RU est modifié en ce sens (*cf.* art. 4 ch. 3 RU).

La formulation suivante est proposée : « Les données enregistrées sont automatiquement détruites après 10 jours. 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 ».

7. Informations aux personnes sous vidéosurveillance

Le requérant est rendu attentif au fait que, dans la mesure où il filme ses employé-e-s, ils doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne.

Une information est faite aux élèves, respectivement les représentants légaux des élèves mineurs.

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

Un article relatif au droit d'accès est 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) ».

---

[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).

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 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.). Le RU prévoit que la clause de confidentialité lui est annexée (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 **Collège du Sud**, Rue de Dardens 79, 1630 Bulle

par

le Collège du Sud,

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

- préavis **partiellement défavorable** à la demande d'installation des caméras **n° 4 à n° 9** avec enregistrement ;
- préavis **défavorable** à la demande d'installation des caméras **n° 1 à n° 3** avec enregistrement ;

aux conditions suivantes :

a. *analyse des risques* : l'organe responsable réévalue 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 caméras 4 à 9. L'ensemble des champs de vision définitifs est communiqué à la Préfecture pour une appréciation définitive. Le nombre de caméra est adapté. Le RU est modifié en ce sens.

   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 ; d'un chiffre expliquant que les images sont enregistrées sur détection de mouvement ; et d'un chiffre expliquant que toute fonctionnalité permettant d'émettre et/ou enregistrer des sons n'est pas autorisée.

c. *signalement* : l'article 1 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 ».

d. *finalité des* données : le but de l'installation mentionné à l'article 1 chiffre 3 RU est modifié de la manière suivante : « lutter contre les actes de déprédations sur les bâtiments et dans l'enceinte du Collège du Sud et contribuer à la poursuite et à la répression d'infractions ».

e. *sécurité des données* : l'organe responsable est la Direction du Collège du Sud. L'article 2 chiffre 1 RU est adapté.

   L'article 2 chiffre 2 RU parle de « flux direct ». Dès lors que seul l'enregistrement est requis, le RU doit être modifié. La gestion des accès est précisée selon la fonction, les besoins et les rôles des personnes. L'article 2 RU est modifié en ce sens.

   L'autorisation ainsi que les droits d'accès y relatifs doivent être distingués selon les fonctions et rôles des personnes (accès aux enregistrements, autorisation d'extraction, accès au serveur, etc.). Ces éléments doivent figurer dans le RU (art. 5). L'accès aux enregistrements est autorisé uniquement en cas d'atteinte avérée. Les utilisateurs changent régulièrement leurs mots de passe. Ainsi une double

authentification est recommandée. Le RU est modifié en ce sens. À l'article 5 chiffre 5, 2ème et 3ème tiret, RU, un lien vers l'article 2 chiffre 2 RU est ajouté.

Des informations complémentaires sont fournies concernant le cache confidentiel (les modalités et fonctionnalités), l'hébergement local des données et la localisation du serveur local.

Le réseau utilisé est distinct de celui de l'école. L'article 5 RU est modifié en ce sens.

En cas de sous-traitance et pour être conforme aux exigences des art. 18 et 12*b* al. 1 let. b LPrD, un contrat particulier doit être conclu contenant les informations citées plus haut ; les mots de passe doivent être changés régulièrement ; une double authentification est recommandée ; l'accès au serveur local ainsi qu'au lieu d'hébergement des enregistrements et/ou données extraites est réservé aux personnes autorisées (*cf.* art. 2 ch. 2 RU). Les informations relatives au lieu d'hébergement des données, les mesures techniques (chiffrement, détenteur de la clé) font l'objet d'une analyse spécifique ; toute fonctionnalité permettant d'émettre et/ou d'enregistrer des sons ne doit pas être utilisée. La clé de chiffrement doit être en main de l'organe responsable, voire d'une des personnes autorisées (art. 2 ch. 2 RU). L'article 5 chiffre 3 lettre a est modifié en ce sens.

f. *destruction des images* : l'article 4 chiffre 3 RU doit déclarer qu'il incombe aux responsables de s'informer régulièrement de la situation au CSUD. Ainsi, les données enregistrées doivent être détruites après 10 jours. En cas d'atteintes avérées, les enregistrements peuvent être conservées jusqu'à 100 jours.

g. *informations aux personnes sous vidéosurveillance :* les collaboratrices et collaborateurs doivent être informés des endroits sous vidéosurveillance et des horaires où le système fonctionne. Les élèves, respectivement les représentants légaux des élèves mineurs, sont également informés.

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

i. *clause de confidentialité :* le prestataire mandaté ainsi que ses collaboratrices et collaborateurs signent une clause de confidentialité dans la mesure où il s'agit de données sensibles et soumises au secret de fonction.

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

V. Remarques

> **Le requérant est rendu attentif au fait que si il filme ses employé-e-s, il est soumis aux règles de la Loi fédérale du 19 juin 1992 sur la protection des données (RS 235.1 ; LPD). Un renvoi est fait à la prise de position du PFPDT sur le sujet (cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/technologien/videoueberwachung/explications-sur-la-videosurveillance-sur-le-lieu-de-travail.html), de laquelle il ressort notamment que les caméras vidéo doivent être orientées et cadrées de sorte que le personnel ne soit pas constamment filmé. Les employés doivent avoir connaissent des zones filmées.**

> 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).

> 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
—
- dossier et compléments en retour
- formulaire de demande signé