



Projet de règlement sur l'organisation des établissements et le statut du personnel pénitentiaires (art. 12 et 21 à 23)

Avis du 10 novembre 2016

Mots clés: projet de règlement, établissement de détention, vidéosurveillance, protection des données personnelles

Contexte: Par courrier électronique du 2 novembre 2016, Mme Nora Krausz, Directrice juridique au Département de la sécurité et de l'économie (DSE) a soumis pour avis au Préposé cantonal à la protection des données et à la transparence (ci-après PPDT) un projet de règlement sur l'organisation des établissements et le statut du personnel pénitentiaires. Ce projet a été soumis à l'attention du PPDT en raison de la présence de plusieurs dispositions portant sur la protection des données personnelles et la vidéosurveillance (art. 12 et 21 à 23).

Bases juridiques: art. 56 al. 3 let. e LIPAD; art. 23 al. 8 RIPAD

Le projet de loi (PL 11 661) sur l'organisation des établissements et le statut du personnel pénitentiaires (LOPP; RSGE F 1 50) est actuellement à l'examen devant le Grand Conseil. Il étend son champ d'application à l'Office cantonal de la détention (OCD) et aux établissements pénitentiaires qui lui sont rattachés. Le projet de règlement soumis au Préposé cantonal devrait entrer en vigueur en même temps que la loi à une date qui reste à déterminer en 2017.

En date du 6 octobre 2016, la Préposée adjointe a rencontré la directrice juridique du DSE afin d'examiner l'avant-projet de règlement. Lors de cette séance, elle a pris connaissance du projet de loi. S'agissant de la vidéosurveillance, elle a observé que l'art. 8 du PL 11 661 reprend en bonne partie une formulation que l'on trouve à l'art. 61 figurant dans la loi sur la police du 9 septembre 2014 (LPol; RSGE F 1 05).

Selon l'art. 8 :

" 1 Les établissements sont équipés de caméras, à l'exception notamment des locaux utilisés exclusivement par le personnel pénitentiaire.

2 Les images filmées peuvent être conservées jusqu'à 100 jours avant d'être détruites, sauf décision émanant d'une autorité compétente par laquelle ce délai est prolongé. Les modalités de visionnement des images filmées sont précisées par voie réglementaire."

Le PL 11 661 ne contient pas d'autres dispositions traitant de la protection des données personnelles. Seul l'art. 9 du projet de loi rappelle le devoir de réserve et le secret de fonction du personnel pénitentiaire dans les limites posées par la LIPAD en matière de d'information du public (règles relatives à la transparence).

Dispositions réglementaires soumises à l'attention du Préposé cantonal

L'art. 12 du règlement rappelle la nécessité de veiller au respect des principes généraux de protection des données prévus par la LIPAD et précise que c'est à la direction de l'OCD qu'il appartient de définir les droits d'accès aux données personnelles conformément aux missions exercées par les différents membres du personnel.

Art. 12 Protection des données personnelles et droits d'accès informatiques

Protection des données personnelles

1 La direction générale et les établissements veillent au respect des principes généraux de protection des données conformément à la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001.

2 La direction générale définit, en collaboration avec les établissements, les droits d'accès aux données personnelles, en adéquation avec les tâches exercées par les membres du personnel pénitentiaire.

Droits d'accès informatiques

3 La direction générale définit, en collaboration avec les établissements, les règles en matière de droit d'accès du personnel pénitentiaire aux applications et aux services informatiques.

Le chapitre III de la loi répond à l'exigence posée par l'art. 8 al. 2 dernière phrase du PL 11 661 de déterminer les modalités de visionnement. Les articles en question détaillent ainsi les mesures à prendre.

A cet égard, les articles 21 à 23 précisent:

- que les établissements exploitent le dispositif de vidéosurveillance et les directions en sont responsables;
- l'exigence d'un signalement adéquat;
- que le contrôle du personnel en temps réel est interdit et que le positionnement des caméras de vidéosurveillance doit être tel que les membres du personnel n'entrent pas en permanence dans le champ des caméras;
- les lieux dans lesquels aucune caméra ne peut être installée (ceux réservés au personnel et les locaux dédiés aux consultations médicales) ou les locaux dans lesquels la vidéosurveillance doit respecter la confidentialité des échanges entre les avocats et les détenus;
- le délai de sept jours dans lequel les images doivent être détruites (délai que l'on retrouve dans la LIPAD);
- les personnes habilitées à ordonner la conservation de certaines images dans des cas bien définis (violence à l'égard du personnel, usage de la force, requête du Ministère public, de la hiérarchie ou de l'inspection générale des services);
- allégation de mauvais traitements et contexte de rixes ou autres violences;
- les personnes habilitées à visionner les images;
- les modalités de conservation des images.

Il est utile de relever également que ces dispositions du chapitre III s'inspirent largement de plusieurs dispositions (art. 18 à 20) du règlement sur l'organisation de la police, du 16 mars 2016 (ROPol; RSGE F 1 05.01), au sujet duquel le Préposé cantonal n'a pas été consulté.

Chapitre III Vidéosurveillance

Art. 21 Principe

Les établissements exploitent le dispositif de vidéosurveillance mis à leur disposition.

Art. 22 Conditions et restrictions

1 *L'utilisation d'un dispositif de vidéosurveillance est clairement signalée.*

2 *L'utilisation de la vidéosurveillance aux seules fins de contrôle en temps réel des activités du personnel est interdite.*

3 *Les locaux strictement réservés au personnel, tels les bureaux, la centrale, la cafétéria, les vestiaires, les salles de repos, les locaux sanitaires ou les couloirs administratifs sans accès direct sur une zone de détention, ne peuvent pas être dotés de caméras de surveillance.*

4 Toutes les dispositions nécessaires sont prises afin que, dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel pénitentiaire, dans toute la mesure du possible, ne se trouvent pas de manière permanente dans le champ des caméras.

5 Les locaux uniquement dédiés à des consultations médicales ne peuvent pas être dotés de caméras de vidéosurveillance.

6 La vidéosurveillance des locaux utilisés par les avocats des personnes détenues doit respecter la confidentialité des échanges et le secret professionnel. Elle n'inclut pas de dispositif audio et ne doit pas permettre de reconnaître les documents examinés par les occupants.

Art. 23 Enregistrement et conservation des images

1 La direction de l'établissement est responsable de la vidéosurveillance.

2 Les enregistrements automatiques d'images de vidéosurveillance sur les serveurs internes aux établissements sont détruits, en principe dans un délai de 7 jours. Pour des besoins opérationnels immédiats, l'opérateur du dispositif de vidéosurveillance peut accéder aux images de la dernière heure enregistrée.

3 La direction de l'établissement ou les membres du personnel pénitentiaire gradés désignés par elle ordonnent la conservation des images enregistrées, en particulier :

- a) lorsqu'un membre du personnel pénitentiaire est victime de violences;
- b) lors d'usage de la force par le personnel pénitentiaire;
- c) sur requête du Ministère public, de la police ou de l'inspection générale des services;
- d) lorsqu'une allégation de mauvais traitement parvient à leur connaissance, notamment sous la forme d'un constat de lésions traumatiques ou d'un signalement par le lésé, par un membre du personnel pénitentiaire ou par un tiers;
- e) lors de rixes, de violences ou de toute autre situation analogue qui le requiert.

4 Les images conservées en vertu de l'alinéa 3 peuvent être sauvegardées jusqu'à 100 jours sur un support approprié. A l'issue de ce délai, elles doivent être détruites, sauf décision contraire d'une autorité compétente.

5 Sauf dans le cas d'investigations entreprises en application du code de procédure pénale suisse, du 5 octobre 2007, seules la direction générale, la direction de l'établissement et les personnes désignées par elles peuvent procéder au visionnement des images sauvegardées. Elles décident des suites à donner.

6 La direction de l'établissement conserve la trace des enregistrements sauvegardés, des visionnements effectués, de l'identité des personnes les ayant traités, ainsi que des remises d'images aux autorités compétentes. Ces informations sont protégées par des moyens appropriés. La direction générale peut y accéder.

7 Les enregistrements sont identifiés par date et événement et sont mentionnés dans le rapport afférent à l'incident.

Principes posés par la LIPAD en matière de vidéosurveillance

A Genève, l'art. 42 ci-après de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; RSGE A 2 08) stipule que la création et l'exploitation d'un système de vidéosurveillance ne sont licites que si, cumulativement, les conditions suivantes sont remplies :

- La vidéosurveillance est propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant;
- L'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions;

- Le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci;
- Dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié.

Art. 42 Vidéosurveillance

1 Dans la mesure où elles ne sont pas dictées par l'accomplissement légal de tâches au sens de l'article 35, la création et l'exploitation d'un système de vidéosurveillance ne sont licites que si, cumulativement :

- a) la vidéosurveillance est propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de dégradations et en contribuant à l'établissement des infractions commises le cas échéant;*
- b) l'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions;*
- c) le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci;*
- d) dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié.*

2 L'éventuel enregistrement de données résultant de la surveillance doit être détruit en principe dans un délai de 7 jours. Ce délai peut être porté à 3 mois en cas d'atteinte avérée aux personnes ou aux biens et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure.

3 Les responsables des institutions prennent les mesures organisationnelles et techniques appropriées afin de :

- a) limiter le visionnement des données, enregistrées ou non, à un cercle restreint de personnes dûment autorisées, dont la liste doit être régulièrement tenue à jour et communiquée au préposé cantonal;*
- b) garantir la sécurité des installations de surveillance et des données éventuellement enregistrées.*

4 En dérogation à l'article 39, la communication à des tiers de données obtenues au moyen d'un système de vidéosurveillance ne peut avoir lieu que s'il s'agit de renseigner :

- a) les instances hiérarchiques supérieures dont l'institution dépend;*
- b) les autorités judiciaires, soit aux conditions de l'article 39, alinéa 3, soit aux fins de dénoncer une infraction pénale dont la vidéosurveillance aurait révélé la commission.*

L'art. 16 du règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 21 décembre 2011 (RIPAD; A 2 08.01), complète l'art. 42 LIPAD. Il traite précisément de la planification (al. 1), la commission consultative de sécurité municipale (al. 2), l'interconnexion entre systèmes de surveillance (al. 3 et 4), l'inventaire (al. 5 et 6), les établissements scolaires (al. 7), la surveillance du trafic routier (al. 8), la délégation à un tiers (al. 9) et les statistiques (al. 10 à 12).

Art. 16 Vidéosurveillance (art. 42 de la loi)

Planification

1 Dans le cadre de ses missions légales de maintien de l'ordre et de la sécurité publique, le Conseil d'Etat, sur proposition du département de la sécurité, de la police et de l'environnement, planifie la vidéosurveillance sur le domaine public du canton.

Commission consultative de sécurité municipale

2 Le département de la sécurité, de la police et de l'environnement informe la commission consultative de sécurité municipale instaurée par l'article 12 de la loi

sur les agents de la police municipale, les contrôleurs municipaux du stationnement et les gardes auxiliaires des communes, du 20 février 2009, des décisions du Conseil d'Etat.

Interconnexion entre systèmes de vidéosurveillance

3 Toute institution publique exploitant un système de vidéosurveillance sur le domaine public peut autoriser une autre institution publique disposant d'ores et déjà d'un système de vidéosurveillance à utiliser les caméras dont elle est la détentrice. L'utilisation des caméras par l'institution publique requérante doit se faire dans le respect des buts de son propre système de vidéosurveillance.

4 La police cantonale peut être autorisée à accéder à tous les systèmes de vidéosurveillance des institutions publiques, que ceux-ci filment ou non le domaine public.

Inventaire

5 La police cantonale tient et met à jour un inventaire et une cartographie des systèmes de vidéosurveillance installés par les institutions de droit public dont le champ de surveillance porte sur le domaine public.

6 Outre les zones placées sous vidéosurveillance, l'inventaire mentionne pour chaque dispositif répertorié :

- a) la finalité de la vidéosurveillance;
- b) l'enregistrement ou non des images et sa durée de conservation;
- c) le type de visionnement qu'implique le dispositif (en direct ou en différé);
- d) le cercle et le statut des personnes autorisées à visionner les images.

Etablissements scolaires

7 Une institution publique exploitant une installation de vidéosurveillance destinée à la protection du patrimoine administratif ne peut filmer un établissement scolaire ou ses abords immédiats durant les heures des activités scolaires et parascolaires, sauf autorisation expresse contraire du département de l'instruction publique, de la culture et du sport.

Surveillance du trafic routier

8 Les caméras affectées à la vidéosurveillance du trafic routier n'enregistrent pas les images en continu mais peuvent procéder à des enregistrements ponctuels, aux fins d'analyses et d'études du trafic. Elles constituent un système de vidéosurveillance sur le domaine public.

Délégation à un tiers

9 La délégation à un tiers par l'institution publique exploitant le système de surveillance de l'enregistrement de la visualisation des images ou d'une manière générale de l'exploitation du système de vidéosurveillance n'est licite que moyennant l'accord préalable des instances dirigeantes de l'institution publique responsable, et pour autant que les conditions cumulatives suivantes soient remplies :

- a) le système satisfait aux exigences de l'article 42 de la loi et à celles du présent règlement;
- b) l'institution publique ne dispose pas du personnel qualifié à ces fins alors que le système de vidéosurveillance est indispensable à la prévention
- c) d'agressions ou de déprédations;
- d) le délégataire est la police cantonale, moyennant une convention passée avec celle-ci au préalable, ou à défaut, une entreprise de sécurité au sens du
- e) concordat sur les entreprises de sécurité, du 18 octobre 1996, qui en remplit les conditions légales.

Statistiques

10 Toute institution publique exploitant un système de vidéosurveillance est tenue de tenir des statistiques, mises à jour semestriellement, sur le nombre d'atteintes aux personnes, y compris à son personnel propre, ou aux biens dont elle est la victime.

11 La République et canton de Genève est considérée comme une seule et unique institution publique aux fins de l'application de l'alinéa 1; la police cantonale tient les statistiques visées par cette disposition, qui portent également sur les atteintes à des tiers.

12 En ce qui concerne les caméras affectées à la vidéosurveillance du trafic routier, le département chargé de la surveillance du trafic tient une statistique séparée de ce mode d'utilisation.

Les recommandations du Préposé fédéral concernant la vidéosurveillance dans le secteur privé

Selon le Préposé fédéral à la protection des données et à la transparence (<http://www.edoeb.admin.ch/datenschutz/00628/00653/00654/index.html?lang=fr>), les systèmes de vidéosurveillance ne sont autorisés qu'à condition qu'ils respectent **les principes de licéité et de proportionnalité**. Chaque système de vidéosurveillance doit concrètement remplir les conditions suivantes:

- La vidéosurveillance ne peut être effectuée que si les personnes filmées ou susceptibles de l'être y consentent ou si l'atteinte à la personnalité qu'elle représente est justifiée par un intérêt prépondérant public ou privé ou par la loi (principe de licéité). Dans la pratique, il est généralement impossible de demander leur accord à toutes les personnes filmées pour exploiter un système de vidéosurveillance. Dans le doute, la vidéosurveillance ne doit être effectuée que s'il existe un intérêt privé ou public prépondérant. Tel est le cas d'un dispositif mis en place à des fins de sécurité.
- La vidéosurveillance doit être un moyen adéquat de réaliser le but poursuivi, à savoir la sécurité (notamment la protection contre les atteintes aux personnes ou aux biens). Elle ne peut être pratiquée que si d'autres mesures moins attentatoires à la vie privée, telles que des verrouillages complémentaires, le renforcement des portes d'entrée ou des systèmes d'alarme, s'avèrent insuffisantes ou impraticables. En outre, les atteintes à la sphère privée causées par la vidéosurveillance doivent se trouver dans un rapport proportionné par rapport au but visé (principe de la proportionnalité). Les caméras factices ne traitent certes pas de données personnelles, mais leur présence donne à penser que tel est le cas. Comme les caméras factices peuvent également s'avérer problématiques pour d'autres raisons juridiques (par ex. pour des questions de responsabilité civile), il est déconseillé de les utiliser.

Quant au **système de vidéosurveillance**, il doit être installé de manière à ce que les principes de la proportionnalité, de la bonne foi et de la transparence soient respectés:

- La caméra doit être installée de manière à ce que n'entrent dans son champ que les images strictement conformes au but de la surveillance (principe de la proportionnalité).
- Le responsable du système de vidéosurveillance doit informer les personnes entrant dans le champ des caméras de l'utilisation d'un tel système au moyen d'un avis bien visible. Au cas où les images sont enregistrées sous quelque forme que ce soit, l'avis doit également indiquer auprès de qui les personnes filmées peuvent faire valoir leur droit d'accès si cela ne ressort pas du contexte (principe de la bonne foi et droit d'accès).

Les principes à respecter lors de l'exploitation d'un système de vidéosurveillance sont au nombre de cinq :

- Les données ne peuvent être utilisées que dans le cadre de la protection contre les atteintes aux personnes ou aux biens. Elles ne peuvent donner lieu à d'autres utilisations (principe de la finalité).
- Le responsable du système de vidéosurveillance doit prendre les mesures organisationnelles et techniques appropriées pour protéger les données personnelles contre tout traitement non autorisé (sécurité des données). Lorsque les images sont transmises par radiocommunication de la caméra au lieu d'enregistrement, le signal doit être crypté ou protégé par d'autres mesures adéquates à même de garantir que des

personnes non autorisées ne puissent pas intercepter le signal et visionner les images.

- Le nombre des personnes qui ont accès aux images - que celles-ci soient diffusées en direct ou enregistrées - doit être aussi restreint que possible (sécurité des données et proportionnalité). Il faut en outre déterminer si le but poursuivi par la vidéosurveillance requiert une surveillance en direct ou s'il suffit que les données vidéo enregistrées soient évaluées suite à un événement. Si la seconde option prévaut, les images ne peuvent être visionnées qu'après qu'un événement se soit produit.
- Les données personnelles enregistrées ne doivent pas être divulguées, sauf si les images sont remises à des fins de dénonciation aux autorités de poursuite pénale ou dans des cas prévus ou autorisés par la loi, par exemple lorsqu'un juge en fait la demande (principe de la finalité).
- Les données personnelles enregistrées par une caméra doivent être effacées dans un délai particulièrement bref. Plus les images sont conservées longtemps, plus les exigences en matière de sécurité des données sont élevées. Toute prolongation de la durée de conservation doit être compensée par l'utilisation de technologies permettant de protéger les données (p. ex. brouillage) et par le cryptage des images enregistrées. Le responsable du système de vidéosurveillance doit, lorsqu'elles le demandent, renseigner toutes les personnes entrées dans le champ de la caméra sur les images les concernant.

Appréciation

Même si cela ne représente que quelques jours de différence, le Préposé cantonal regrette que la loi sur la police et le projet de LOPP se soient écartés du délai maximal de trois mois fixés par la LIPAD au terme desquels les images de vidéosurveillance doivent être détruites en prévoyant un délai maximal de 100 jours.

Les établissements pénitentiaires doivent être formés et informés sur la destruction effective des images à l'échéance de ce délai légal. Quelques cas rencontrés dans la pratique ont montré au Préposé cantonal que ce n'était pas systématiquement le cas.

Ces deux aspects ne relèvent toutefois pas de l'analyse du présent projet de règlement. Sur ce point, la Préposée adjointe observe que les remarques évoquées lors de la rencontre du 6 octobre 2016 ont bien été intégrées et en remercie le département.

Le fait que le règlement détaille les conditions d'exploitation de systèmes de vidéosurveillance doit être salué tout en rappelant que les deux dispositions-cadre de la LIPAD (art. 42) et du RIPAD (art. 16) trouvent également application dans cette matière.

Au vu de la formulation de l'art. 22 al. 4 du projet de règlement – qui a le même contenu que l'art. 19 al. 4 ROPol – l'on comprend que des membres du personnel pénitentiaire pourront se trouver presque en permanence dans le champ de certaines caméras de vidéosurveillance. Si tel devait être le cas, l'art. 42 al. 1 lettre d LIPAD précise que les personnes concernées doivent être rendues d'emblée non identifiables par un procédé technique approprié.

En cas d'intérêt, le Préposé cantonal se tient à la disposition de l'OCD pour organiser une formation à l'attention des membres du personnel concerné.

A toutes fins utiles, la Préposée adjointe rappelle l'existence de trois documents qui peuvent être utiles à l'OCD et aux établissements pénitentiaires:

- La fiche info du PPDT "Caméras de vidéosurveillance – aspects juridiques et pratiques", <https://www.ge.ch/ppdt/fiches-info/doc/Cameras-videosurveillance.pdf>
- Les recommandations du Forum genevois de sécurité sur la vidéosurveillance, <http://www.fgsonline.ch/CMS/default.asp?ID=251>

- Le Commentaire du Secrétariat d'Etat à l'économie (seco) relatif à l'art. 26 de l'ordonnance 3 relative à la loi sur le travail - Chapitre 2 - Exigences particulières en matière de protection de la santé - Section 5 - Surveillance des travailleurs, https://www.seco.admin.ch/dam/seco/fr/dokumente/...pdf.../ArGV3_art26_fr.pdf.

* * *

Les Préposés remercient le DSE de les avoir consultés et restent à disposition.

Pascale Byrne-Sutton
Préposée adjointe

Stéphane Werly
Préposé cantonal