



Projet de règlement sur la brigade de sécurité et des audiences

Avis du 27 février 2018

Mots clés: Office cantonal de la détention, pouvoir judiciaire, police, vidéosurveillance, protection des données personnelles, convoyage de détenus

Contexte: dispositions réglant la vidéosurveillance dans le cadre des missions de la brigade de sécurité et des audiences

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

1. Caractéristiques de la demande

Par courrier électronique du 16 février 2018, Mme Nora Krausz, directrice juridique à la direction générale de l'Office cantonal de la détention (Département de la sécurité et de l'économie), a sollicité du Préposé cantonal à la protection des données et à la transparence son avis sur un projet de règlement sur la brigade de sécurité et des audiences, lequel comporte un chapitre sur la vidéosurveillance. Souhaitant déposer le projet "dès que possible" auprès du Conseil d'Etat, la précitée a émis le souhait d'avoir une réponse d'ici au 2 mars 2018.

Mme Nora Krausz a précisé que le projet de règlement a pour principales bases légales le code pénal, ainsi que la loi d'application du code pénal suisse et d'autres lois fédérales en matière pénale (LaCP; RSGe E 4 10).

Il sied en outre de préciser que dans le contexte de la rédaction du règlement dont il est question, des échanges sont intervenus entre Mme Nora Krausz et le Préposé cantonal lors d'une rencontre le 10 juillet 2017. Dans le cadre de ces échanges, le Préposé cantonal a attiré l'attention sur certaines dispositions du règlement qui n'étaient pas compatibles avec la LIPAD. Il constate que des modifications ont été apportées au projet de règlement pour faire suite aux remarques formulées.

Les dispositions du projet de règlement sur la brigade de sécurité et des audiences concernant la protection des données sont les suivantes :

Chapitre III Vidéosurveillance

Art. 12 Principe

¹ *La brigade exploite le dispositif de vidéosurveillance se trouvant dans les locaux du pouvoir judiciaire et de la police dont elle assure la sécurité, ainsi que dans les véhicules qu'elle utilise pour le convoyage des détenus.*

² *Le service de sécurité du pouvoir judiciaire accède en direct aux images provenant du système de vidéosurveillance exploité par la brigade dans les locaux partagés entre les deux entités.*

Art. 13 Conditions et restrictions

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

² *L'utilisation de la vidéosurveillance pour le 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 passage du public, ne peuvent pas être dotés de caméras de vidéosurveillance.

⁴ Toutes les dispositions nécessaires sont prises afin que, dans l'accomplissement de son activité à son poste de travail, le personnel de la brigade, dans toute la mesure du possible, ne se trouve pas de manière permanente dans le champ des caméras.

Art. 14 Enregistrement et conservation des images

¹ Le responsable du service et les membres du personnel de la brigade de sécurité et des audiences qu'il désigne sont responsables de la vidéosurveillance.

² Les enregistrements automatiques d'images de vidéosurveillance sur les serveurs internes sont détruits, dans un délai de 7 jours au plus tôt et de 100 jours au plus tard. Pour des besoins opérationnels immédiats, l'opérateur du dispositif de vidéosurveillance peut accéder aux images de la dernière heure enregistrée, si le dispositif le permet.

³ Le responsable du service et les membres du personnel de la brigade de sécurité et des audiences qu'il désigne ordonnent la conservation des images enregistrées en cas d'atteinte avérée aux personnes ou aux biens, en particulier :

- a) lorsqu'un membre du personnel de la brigade de sécurité et des audiences est victime de violences;
- b) lors d'usage de la force par le personnel de la brigade de sécurité et des audiences;
- c) sur requête du Ministère public ou de la police;
- 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 de la brigade de sécurité et des audiences ou par un tiers;
- e) lors de rixes, de violences, d'évasion, de tentative d'évasion 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 en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure.

⁵ Sauf dans le cas d'investigations entreprises en application du code de procédure pénale suisse, du 5 octobre 2007, seules la direction générale, le responsable du service et les membres du personnel de la brigade de sécurité et des audiences ou du service de sécurité du pouvoir judiciaire qu'il désigne peuvent procéder au visionnement des images sauvegardées. Ils décident des suites à donner.

⁶ Le responsable du service et les membres du personnel de la brigade de sécurité et des audiences qu'il désigne conservent 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 assurant leur confidentialité.

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

2. Les règles relatives à la vidéosurveillance

La vidéosurveillance touche inmanquablement certains **droits fondamentaux**, particulièrement le droit au respect de la sphère privée et la liberté personnelle (art. 10 al. 2 et 13 Cst., 8 CEDH et 19 Pacte II; voir Cour eur. D.H., *Perry*, du 17 juillet 2003), lesquels protègent notamment l'intégrité physique et psychique d'un individu, sa liberté de mouvement, toutes les informations le concernant qui ne sont pas accessibles au public, les données d'identification et la correspondance privée.

Le recours à la **vidéosurveillance doit respecter ces libertés** de manière générale, que ce soit en droit public ou en droit privé (Flückiger Alexandre/Auer Andreas, La vidéosurveillance dans l'œil de la Constitution, PJA 2006, p. 926).

Les conditions de restrictions de ces libertés sont énumérées à l'art. 36 Cst. Sont exigés: une base légale, un intérêt public et le respect de la proportionnalité et de l'essence des droits fondamentaux.

Suite à l'arrêt rendu par le Tribunal fédéral en la cause 1C_315/2009, du 13 octobre 2010, il convient de préciser que, si une base légale matérielle suffit pour l'installation d'un dispositif de vidéosurveillance qui ne permette pas l'enregistrement des images, une **base légale formelle** est nécessaire pour l'installation d'un dispositif qui le permette.

A Genève, cette base légale formelle est l'art. 42 de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; A 2 08), faute d'une disposition légale plus spécifique. Cette disposition prévoit que:

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 déprédations 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).

Finalement, il convient de citer les **recommandations du Préposé fédéral concernant la vidéosurveillance dans le secteur privé**¹, selon lesquelles 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.

3. Appréciation

Le projet de règlement sur la brigade de sécurité et des audiences prévoit à ses articles 12 à 14 des dispositions concernant la vidéosurveillance. Il convient d'examiner si ces dispositions sont conformes aux deux dispositions-cadre de la LIPAD (art. 42) et du RIPAD (art. 16) qui trouvent également application dans cette matière, dès lors que le Département de la sécurité et de l'économie et le Pouvoir judiciaire sont des institutions publiques soumises à la LIPAD (art. 3 al. litt. a).

L'article 12 consacre le principe de l'exploitation d'un dispositif de vidéosurveillance par la brigade de sécurité et des audiences, ainsi que l'accès en direct à certaines de ces images par le service de sécurité du pouvoir judiciaire. Cette disposition n'appelle pas de commentaires particuliers.

¹<https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/dokumentation/feuilles-thematiques/videosurveillance-effectuee-par-des-particuliers.html>

Le Préposé cantonal salue le fait que l'article 13 du projet prévoit, comme le requiert l'article 42 LIPAD, que l'existence du système de vidéosurveillance est signalée et que l'emplacement des caméras de vidéosurveillance est exclu des locaux strictement réservés au personnel. De même, il remarque qu'il est prévu que *"toutes les dispositions nécessaires sont prises afin que, dans l'accomplissement de son activité à son poste de travail, le personnel, dans toute la mesure du possible, ne se trouve pas de manière permanente dans le champ des caméras"*. S'agissant de ce dernier point, dans les situations où il serait absolument impossible d'éviter qu'un membre du personnel se trouve dans le champ de la caméra, il conviendrait alors de le rendre non identifiable (visage flouté par exemple).

L'article 14 al. 2 à 4 du projet traite de la conservation des images. Le Préposé cantonal remarque qu'il est prévu à l'alinéa 2 que les enregistrements *"sont détruits, dans un délai de 7 jours au plus tôt et de 100 jours au plus tard"*. Il considère qu'il aurait été préférable d'opter pour une formulation prévoyant une durée de conservation des images de 7 jours, sauf en cas d'atteinte avérée aux personnes et aux biens auquel cas le délai peut être porté à 3 mois, comme le prévoit l'article 42 al. 2 LIPAD.

Le projet de règlement prévoit à ses articles 14 al. 3 et 4 que les images conservées en cas d'atteinte avérée aux personnes et aux biens peuvent être sauvegardées 100 jours et qu'à l'issue de ce délai, elles doivent être détruites sauf en cas d'ouverture d'une information pénale, cas où elles peuvent être sauvegardées jusqu'à l'issue de la procédure. Cette disposition, malgré une différence avec le délai de 3 mois (plutôt que 100 jours) prévus par la LIPAD, est conforme à la jurisprudence du Tribunal Fédéral. En effet, selon la jurisprudence, une durée de cent jours, même si elle représente une atteinte non négligeable aux droits fondamentaux des personnes concernées, est admissible, du moment que les enregistrements issus de la surveillance litigieuse sont exclusivement utilisés dans le cadre d'une procédure pénale (ATF 133 I 88; voir également Cour eur. D.H., Amann, du 16 février 2000).

Par contre, la marge de manœuvre importante (entre 7 et 100 jours) laissée par l'article 14 al. 2 du projet dans toutes les autres situations est peu compatible avec les exigences de la LIPAD et de la jurisprudence susmentionnée, au regard du principe de la proportionnalité.

A cet égard, le Préposé cantonal relève qu'en matière pénitentiaire ou de police à Genève, les textes suivants traitent explicitement de la durée de conservation des images de vidéosurveillance: la loi sur la police (LPol; F 1 05) prévoit à son article 61 al. 2 que *"les images filmées sont conservées durant 100 jours avant d'être détruites, sauf décision émanant d'une autorité compétente par laquelle ce délai est prolongé"* et le Règlement sur l'organisation des établissements et le statut du personnel pénitentiaires (ROPP; F 1 50.01) dispose à son article 23 al. 2 que *"les enregistrements automatiques d'images de vidéosurveillance sur les serveurs internes aux établissements sont détruits, dans un délai de 7 jours au plus tôt et de 100 jours au plus tard"*. Le projet de règlement dont il est question reprend donc le texte de cette dernière disposition. Si le Préposé cantonal comprend parfaitement l'intérêt d'une certaine harmonisation des normes en la matière ainsi que la volonté de conserver les images aussi longtemps que le dépôt d'une plainte pénale est possible, il regrette le flou laissé dans la conservation d'enregistrements lorsqu'il n'y a pas d'atteinte avérée aux personnes ou aux biens, flou peu compatible avec le respect du principe de la proportionnalité. Il encourage dès lors vivement la destruction dans un délai de 7 jours des enregistrements qui ne sont pas visés par l'article 14 alinéas 3 et 4 du projet et, en conséquence, de revoir la formulation de l'article 14 al. 2 du projet.

L'article 14 al. 5 désigne les personnes qui peuvent procéder au visionnement des images. Il convient que le nombre de membres désignés par le responsable du service pour procéder au visionnement soit aussi restreint que possible, comme le commande l'article 42 al 3 litt. a LIPAD. Cette dernière disposition exige également que la liste (ou la

fonction) de ces personnes soit régulièrement tenue à jour et communiquée au Préposé cantonal.

Les autres alinéas n'appellent pas de commentaires particuliers.

Le Préposé cantonal remercie finalement Mme la directrice juridique à la direction générale de l'Office cantonal de la détention des changements d'ores et déjà effectués suite à leur rencontre du 10 juillet 2017.

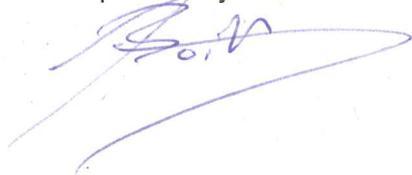
4. Avis du Préposé cantonal

En conclusion, à la vue des éléments ci-dessus, le Préposé cantonal encourage la direction générale de l'Office cantonal de la détention à revoir la formulation de l'art. 14 al. 2 du règlement afin d'assurer plus clairement le respect du principe de la proportionnalité.

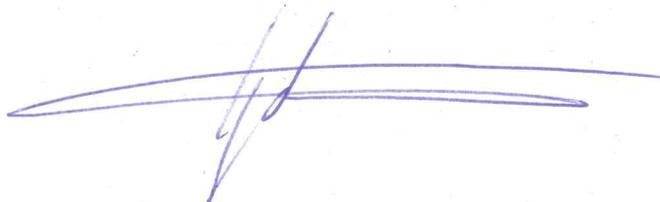
Pour le surplus et moyennant le respect lors de l'application pratique du règlement des remarques susmentionnées, le projet est compatible avec la protection des données.

Le Préposé cantonal remercie en outre la direction générale de l'Office cantonal de la détention de l'avoir consulté. Il rappelle enfin l'obligation de déclarer au catalogue les fichiers de données personnelles détenues par les institutions publiques (art. 43 LIPAD et art. 18 RIPAD).

Joséphine Boillat
Préposée adjointe

A handwritten signature in blue ink, appearing to be 'J. Boillat', written over a horizontal line.

Stéphane Werly
Préposé cantonal

A handwritten signature in blue ink, appearing to be 'S. Werly', written over a horizontal line.