Département de la sécurité, de la population et de la santé (DSPS) – Office cantonal de la détention – Utilisation de "bodycams"

Avis du 10 octobre 2022

Mots clés: Données personnelles, données personnelles sensibles, vidéosurveillance, "bodycams", établissements pénitentiaires, base légale, proportionnalité

Contexte: Utilisation de "bodycams" au sein des établissements pénitentiaires genevois

Bases juridiques: art. 56 al. 3 litt. c LIPAD

1. Contexte

Le Préposé cantonal à la protection des données et à la transparence (PPDT) a été sollicité concernant l'utilisation de "bodycams" au sein des établissements pénitentiaires genevois, plus particulièrement concernant la conformité de l'utilisation des "bodycams" avec le cadre juridique actuel.

2. Bases légales

Le cadre international

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ou "Convention 108")[1], dont l'objectif central est de lutter contre les abus dans la collecte de données personnelles, définit un certain nombre de principes qu'il appartient aux Etats de transposer dans leur droit interne. Une nouvelle teneur de ce traité (désormais Convention 108+) devrait prochainement entrer en vigueur, ce qui impliquera une adaptation de la LIPAD.

La Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données[2] fixe des normes minimales pour le traitement des données à des fins policières au sein de chaque Etat membre. En exécution de ce texte, la Suisse s'est dotée d'une loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal, du 28 septembre 2018, entrée en vigueur le 1er mars 2019[3].

[1] RS 0.235.1.
[2] JO L 119 du 4 mai 2016, pp. 89 ss.
[3] LPDS; RS 235.3.

Le travail de transposition prescrit est actuellement en cours à Genève dans le cadre de la révision de la LIPAD.

Les règles constitutionnelles

A titre liminaire, il sied de rappeler qu'en matière de vidéosurveillance, plusieurs libertés peuvent être en jeu: la liberté personnelle, et plus particulièrement la garantie de l'intégrité physique et psychique (art. 10 al. 2 Cst.), le droit au respect de la sphère privée (art. 13 al. 1 Cst. et 8 CEDH) et encore le droit d'être protégé contre l'emploi abusif des données personnelles (art. 13 al. 2 Cst.)[4].

Conformément à l'art. 36 Cst., les restrictions aux libertés ne sont conformes à la Constitution que lorsqu'elles peuvent s'appuyer sur une base légale, sont justifiées par un intérêt public ou par la protection des droits fondamentaux d'autrui et sont proportionnées au but visé.

La constitutionnalité des systèmes de vidéosurveillance doit donc être examinée à l'aune des principes susmentionnés.

La LIPAD

L'enregistrement d'images par un dispositif de vidéosurveillance permettant d'identifier des personnes déterminées tombe dans le champ d'application des lois sur la protection des données, ce qu'a confirmé le Tribunal fédéral[5].

Les règles posées par la LIPAD concernant la collecte et le traitement de données personnelles sont les suivantes :

Notion de données personnelles et de données personnelles sensibles

Par données personnelles, il faut comprendre : « toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable » (art. 4 litt. a LIPAD).

Par données personnelles sensibles, on entend les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles, la santé, la sphère intime ou l'appartenance ethnique, des mesures d'aide sociale, des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

Principes généraux relatifs à la protection des données

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 38 LIPAD) :

- Base légale (art. 35 al. 1 et 2 LIPAD)

Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, des données personnelles sensibles ne peuvent être traitées que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée.

- Bonne foi (art. 38 LIPAD)

[4] Pour plus de détails sur les libertés en jeu, voir Alexandre Flückiger et al., Vidéosurveillance et risques dans l'espace à usage public: représentations des risques, régulation sociale et liberté de mouvement, CETEL, Genève 2006, pp. 49 ss.
[5] Arrêt du Tribunal fédéral 4A_576/2015, du 29 mars 2016, consid. 2.2.1.

Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

- Proportionnalité (art. 36 LIPAD)

En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

- Finalité (art. 35 al. 1 LIPAD)

Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi.

- Reconnaissabilité de la collecte (art. 38 LIPAD)

La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

- Exactitude (art. 36 LIPAD)

Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

- Sécurité des données (art. 37 LIPAD)

Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

- Destruction des données (art. 40 LIPAD)

Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi. Ce dernier principe touche précisément le droit à l'oubli, selon lequel, dans un cas particulier, certaines informations n'ont plus à faire l'objet d'un traitement par l'institution publique concernée.

Règles en matière de vidéosurveillance

L'art. 42 LIPAD 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.

Cette disposition est complétée par l'art. 16 RIPAD.

La loi sur l'organisation des établissements et le statut du personnel pénitentiaires (LOPP) et son règlement d'application

L'art. 8 prévoit que les établissements sont équipés de caméras, à l'exception notamment des locaux utilisés exclusivement par le personnel pénitentiaire. La durée de conservation des images filmées est fixée à 100 jours avant qu'elles ne soient détruites, sauf décision émanant d'une autorité compétente par laquelle ce délai est prolongé. En outre, il est indiqué que les modalités de visionnement des images filmées sont précisées par voie réglementaire.

L'exposé des motifs relatif au PL 11661 précisait ce qui suit au sujet de cette disposition : "*Cet article permet d'ancrer dans une base légale formelle le fait que les locaux utilisés exclusivement par le personnel pénitentiaire ne peuvent être soumis à vidéosurveillance. D'autres lieux pourront être visés et seront, le cas échéant, déterminés par voie réglementaire ou de directive. Il permet également de prévoir que les images puissent être conservées d'office jusqu'à 100 jours, en dérogation au délai prévu à l'article 42, alinéa 2, de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (A 2 08, LIPAD). Cette dernière loi s'applique pour le surplus*".

Les art. 21 à 23 ROPP régissent les modalités de la 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 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 détention, ne peuvent pas être dotés de caméras de vidéosurveillance.
[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, 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.
[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 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 pénitentiaire ou par un tiers;
e) lors de rixes, de violences ou de toute autre situation analogue qui le requiert;
f) en cas de sanction disciplinaire prise à l'encontre d'une personne détenue ou d'un membre du personnel pénitentiaire.
[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.

Par ailleurs, une directive, ainsi que divers ordres de service concernant l'utilisation des "bodycams" ont été adoptés par l'OCD.

Il ressort notamment de la Directive de l'Office cantonal de la détention sur l'utilisation des bodycams (n° 5.04) que:

- Les "bodycams" enregistrent tant l'image que le son et permettent de couvrir des évènements dans des locaux ne disposant pas de système de vidéosurveillance fixe.
- Les "bodycams" sont paramétrées pour enregistrer la séquence dès l'appui sur le bouton de démarrage de l'enregistrement; l'enregistrement du pré-évènement n'est pas activé.
- Une "bodycam" est systématiquement utilisée pour les situations planifiées suivantes: extraction d'une cellule d'une personne détenue récalcitrante ou présentant un danger pour le personnel ou elle-même; mise en cellule forte; mise en cellule forte de soins intensifs; intervention dans le cadre d'une médication sous contrainte.

- Une "bodycam" peut être utilisée en dehors de ces situations sur ordre de la direction ou d'une personne désignée par elle.
- Lorsque la fouille d'une personne détenue "*nécessite une mise à nu en deux temps, le porteur de la bodycam veille à ne pas filmer le sexe de la personne détenue ainsi que la poitrine s'il s'agit d'une femme. Le porteur de la bodycam place sa main sur l'objectif de la caméra durant ce moment de la fouille en deux temps ou se place de manière à garantir l'invisibilité des parties du corps décrites plus haut. En aucun cas la bodycam doit être éteinte lors de cette opération. (…) Toutefois, dans le cas où la personne détenue s'agite au point de mettre en péril la sécurité du personnel présent (perte de maîtrise de la sécurité), le porteur de la bodycam peut intervenir immédiatement en renfort de ses collègues même si cela implique un risque de filmer les parties intimes de la personne détenue*".
- Diverses dispositions ont trait à la sécurité des données, l'extraction des séquences, leur accès et leur transmission.

Finalement, les Préposés ont pris note que, lorsque des enregistrements sont en cours, les personnes détenues en sont informées car les dispositifs émettent un signal lumineux rouge.

3. Appréciation

Les Préposés comprennent que le but de l'utilisation de "bodycams" dans les établissements pénitentiaires est de protéger les membres du personnel et de dissuader les personnes détenues de s'en prendre physiquement à eux. En outre, les images permettent également, en cas de dénonciation au Ministère public, de déterminer le déroulement des faits.

Les Préposés relèvent que les enregistrements qui interviennent dans les établissements pénitentiaires au moyen de "bodycams" sont susceptibles de faire apparaître directement ou indirectement des données personnelles sensibles, de sorte que les exigences prévues par l'art. 35 al. 2 LIPAD en matière de base légale doivent être respectées. Selon cette disposition, "*des données personnelles sensibles ou des profils de la personnalité ne peuvent être traités que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée*". Deux conditions cumulatives sont donc requises: une loi qui définisse clairement la tâche considérée et un traitement qui soit absolument indispensable à l'accomplissement de la tâche. L'alternative au caractère indispensable à l'accomplissement de la tâche est la nécessité du traitement et la présence du consentement. Il est précisé que ces deux critères ne dispensent pas de l'obligation d'avoir une tâche clairement définie dans la loi.

Se pose ici la question de la densité normative exigée en cas de base légale pour le traitement de données personnelles sensibles. En effet, "*la base légale doit non seulement exister pour servir de base à l'activité étatique, mais doit encore présenter un certain contenu, une densité normative suffisante*". Ainsi, la norme doit être suffisamment claire et précise : "*Il s'agit d'éviter le blanc-seing aux autorités d'exécution, qui viderait de son sens l'exigence de légalité*"[6]. Les exigences de densité normative varient en fonction des buts de la norme, de ses effets sur les droits et les obligations des administrés, de la prévisibilité des décisions prises mais, traditionnellement, les exigences sont moins strictes s'agissant de l'administration de prestation, de la gestion du domaine public qu'en cas de restriction de droits fondamentaux, situation qui requiert une densité normative plus grande[7]. En l'espèce, le traitement de données impliqué par l'utilisation de "bodycams" dans les prisons genevoises touche aux droits fondamentaux des personnes concernées, de sorte que les exigences en matière de densité normative doivent être considérées comme élevées. Sur ce

[6] Clémence Grisel Rapin, La légalité, *in* Bellanger François/Bernard Frédéric, Les grands principes du droit administratif, Zurich 2022, p. 43.
[7] Clémence Grisel Rapin, *op. cit.*, p. 48.

dernier point, il est intéressant de noter qu'en France la Commission nationale de l'informatique et des libertés (CNIL), dans sa délibération n°2019-140 du 5 décembre 2019 portant avis sur un projet de décret relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des personnels de surveillance de l'administration pénitentiaire (demande d'avis n° 19020058), a noté que les traitements projetés étaient "*susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment parce qu'ils portent sur des données sensibles*"[8].

Dans un avis du 25 août 2022[9], les Préposés ont considéré que l'utilisation de "bodycams" par la police devait reposer sur une base légale encadrant ce traitement de données personnelles avec clarté: dans quelles situations l'enregistrement peut-il intervenir, quelle information est transmise à la personne filmée et comment, qui peut visionner les images et dans quelles situations. Une base réglementaire n'était pas considérée comme suffisante. Il était par ailleurs relevé que ces prises de vue, mal encadrées, pourraient s'apparenter à de la surveillance de masse.

L'utilisation de "bodycams" dans le domaine pénitentiaire ne saurait, certes, présenter le risque d'une surveillance de masse; toutefois, même si les enjeux sont différents, l'atteinte à la sphère privée et à la personnalité des personnes concernées par l'usage de "bodycams" dans les établissements pénitentiaires est importante, de sorte que la question de la base légale doit être examinée avec attention.

En l'espèce, les bases légales formelles sur lesquelles repose actuellement l'utilisation de "bodycams" au sein des établissements pénitentiaires sont les art. 42 LIPAD et 8 LOPP. Elles sont précisées au niveau réglementaire, ainsi que par des directives et divers ordres de service.

Ainsi, le principe de l'utilisation de systèmes de vidéosurveillance au sein des établissements pénitentiaires repose sur une base légale formelle. La finalité de cette utilisation découle de l'art. 42 LIPAD, à savoir la sécurité des personnes et des biens en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant (art. 42 al. 1 let a LIPAD). Cette disposition vise toutefois la vidéosurveillance de manière générale; les finalités liées spécifiquement à la vidéosurveillance dans les établissements pénitentiaires pourraient être précisées à l'art. 8 LOPP, par exemple, à l'instar de l'art. 32 al. 1 de la loi bernoise sur l'exécution judiciaire du 23 janvier 2018[10]. L'art. 8 LOPP encadre également la durée de conservation des images et décrit les locaux exclus de la surveillance. Par ailleurs, l'art. 42 LIPAD consacre les exigences requises s'agissant des modalités d'installation du système. Finalement, le ROPP encadre l'enregistrement et la conservation des images, ainsi qu'apporte des précisions sur les locaux dans lesquels la vidéosurveillance ne peut être utilisée ou doit être utilisée de manière limitée (art. 22 et 23 ROPP). L'accent de la protection est mis sur les droits des membres du personnel à ne pas être surveillés, les situations de consultation médicale ainsi que sur la communication entre les personnes détenues et leur conseil.

Si le principe de l'utilisation de la vidéosurveillance, de manière générale, dans les prisons, repose sur une base légale formelle, complétée par des normes de niveau réglementaire, qui en prévoient les modalités, les Préposés constatent qu'il n'y a toutefois aucune disposition spécifique relative aux "bodycams", ni de rang légal ni de rang réglementaire. De la sorte, la question qui se pose est de savoir si les bases légales susmentionnées suffisent à l'utilisation de "bodycams" dans les établissements pénitentiaires ou si des bases légales complémentaires sont nécessaires.

[8] https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039690387/, consulté le 29 septembre 2022.
[9] https://www.ge.ch/document/29973/telecharger
[10] LEJ; RSBe 341.1.

Les Préposés relèvent que l'utilisation de "bodycams" pose des problématiques particulières intrinsèques à leur mode de fonctionnement: l'enregistrement est déclenché par celui qui la porte, il peut potentiellement être déclenché en tout lieu et à tout moment, y compris dans des espaces non communs ou lors de situations particulièrement intrusives pour la personne détenue (dans la cellule, lors d'une fouille, comme semble le prévoir la Directive de l'OCD). Ces situations portent une atteinte potentiellement très importante à la sphère privée des personnes détenues; de plus, comme cela a déjà été mentionné, l'on ne peut exclure que des données sensibles apparaissent directement ou indirectement sur les images, de sorte que les exigences de l'art. 35 al. 2 LIPAD en matière de base légale doivent être respectées.

Les Préposés considèrent ainsi que la densité normative requise dans l'élaboration de bases légales relatives à l'utilisation de "bodycams" dans les établissements pénitentiaires n'est pas satisfaite par le droit actuel. Cette utilisation devrait faire l'objet d'une base légale spéciale, dans la LOPP, portant spécifiquement sur l'utilisation de "bodycams" au sein des établissements pénitentiaires genevois. En effet, il sied que figurent au niveau de la base légale formelle le principe de l'utilisation de "bodycams", les finalités de cette utilisation, les situations autorisant le port de "bodycams", ainsi que les situations dans lesquelles l'enregistrement peut/doit intervenir, et sur la base de quels critères. En effet, les bases légales générales en matière de vidéosurveillance (art. 42 LIPAD et art. 8 LOP, ainsi que les dispositions d'application de rang réglementaire) ne sauraient suffire sur ces points qui soulèvent des problématiques spécifiquement liées aux "bodycams". Il peut par contre y être renvoyé s'agissant de la durée de conservation des images, de la consultation de ces dernières et du cadre relatif à la sécurité des données.

Des règlements, voir des directives ou ordres de service reposant sur les bases légales recommandées peuvent ensuite être adoptés afin de préciser les processus pour les membres du personnel concernés et les modalités légalement exigées.

Certaines dispositions figurant actuellement dans la Directive de l'OCD sur l'utilisation de bodycams devraient ainsi figurer dans la loi.

Ceci étant précisé, les Préposés ont également examiné les modalités prévues par la Directive de l'OCD sur l'utilisation de bodycams. Sans être exhaustifs, ils relèvent les éléments suivants:

- Des fouilles de personnes détenues pourraient être filmées. Les Préposés s'en inquiètent au regard du respect de la sphère privée des personnes concernées. Ils relèvent que les mesures pour remédier à ce que des parties intimes des personnes détenues figurent sur les images ne sont pas suffisantes pour pallier le risque d'atteinte à la personnalité. Ils questionnent le principe même de filmer une fouille au regard du respect de la sphère privée et doutent que l'intérêt public à la sécurité ou à l'apport d'une preuve puisse être prépondérant.
- La question de la reconnaissabilité de l'utilisation de la caméra, ainsi que de la communication faite aux personnes concernées, devrait être abordée plus en détail. Un enregistrement à l'insu de la personne concernée devrait être expressément interdit.
- Les données traitées pourraient être précisées (au-delà de l'image et du son).

Au vu de ce qui précède, l'adoption de bases légales idoines apparaît nécessaire aux Préposés. Dans l'optique de l'élaboration d'un projet de loi, ils recommandent la consultation de représentants de toutes les parties concernées.

Les Préposés regrettent qu'aucun projet-pilote n'ait été mené en amont afin de permettre une meilleure analyse de la situation, comprenant une analyse d'impact détaillée en matière de protection des données en vue de l'adoption de bases légales idoines.

4. Conclusion

Au vu de ce qui précède, **les Préposés invitent l'OCD à élaborer un projet de base légale** relative à l'utilisation de "bodycams" dans les établissements pénitentiaires genevois.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal