



Requête en cessation de l'usage de "bodycams" dans les établissements pénitentiaires genevois et en constatation de l'illicéité de ces dispositifs

Recommandation du 26 avril 2023

I. Le Préposé cantonal à la protection des données et à la transparence constate:

1. Dans un courriel daté du 9 décembre 2022 adressé à la responsable LIPAD du Département de la sécurité, de la population et de la santé (DSPS), Me X, mandaté par A et par B, gardien au sein de la prison de Champ-Dollon, a sollicité ce qui suit: *"vu l'illégalité totale du système de bodycams actuellement déployé au sein des prisons genevoises, et notamment Champ-Dollon (...), mes mandants vous prient d'intervenir afin de mettre fin à ce système, avec effet immédiat, et constater la violation des droits des fonctionnaires concernés protégés par la LIPAD"*.
2. Le 4 avril 2023, la responsable LIPAD du DSPS, dès lors qu'elle n'entendait pas faire droit intégralement aux prétentions des requérants, a saisi le Préposé cantonal, conformément à l'art. 49 al. 4 LIPAD. Elle souhaitait son avis sur les points suivants:
 - La requête formulée par Me X est intervenue par courrier électronique, alors que l'art. 49 al. 1 LIPAD indique qu'elle doit être adressée "par écrit"; s'agissant d'une procédure à caractère décisionnel, la responsable LIPAD du DSPS se demande s'il s'agit d'un vice de forme qui doit être corrigé.
 - La qualité pour agir de A est contestée (en référence à l'arrêt ATA/1520/2019), tout comme celle de M. B, puisque ce dernier, de par sa fonction, n'est pas amené à utiliser de bodycams, ni à intervenir dans des situations où il risquerait d'être filmé par ces dispositifs.
 - Sur le fond, un projet de base légale spécifique à l'utilisation des "bodycams" a été établi et est actuellement en consultation auprès des associations représentatives du personnel; de plus, l'art. 8 LOPP constitue une base légale à la vidéosurveillance dans les prisons genevoises, de sorte que le cadre légal actuel est suffisant et qu'il ne se justifie pas d'y mettre un terme.
3. Etaient joints au courrier susmentionné: la directive et l'ordre de service relatifs à la vidéosurveillance dans les prisons genevoises, le cahier des charges générique pour la fonction occupée par M. B, la requête de Me X, ainsi qu'un projet de loi modifiant la loi sur la police impliquant notamment une modification de la LOPP sur la question de la vidéosurveillance.
4. Conformément à l'art. 49 al. 5 LIPAD, *"le Préposé cantonal instruit la requête de manière informelle, puis il formule, à l'adresse de l'institution concernée et du requérant, une recommandation écrite sur la suite à donner à la requête"*.

5. Il sied de préciser que le Préposé cantonal a d'ores et déjà été interpellé concernant l'utilisation des "bodycams" au sein des établissements pénitentiaires genevois, plus particulièrement concernant la conformité de cette utilisation avec le cadre juridique actuel. Dans un avis du 10 octobre 2022 (<https://www.ge.ch/document/ppdt-videosurveillance-avis-droit-du-10-octobre-2022>), il avait invité le DSPP à élaborer un projet de base légale relative à l'utilisation de "bodycams" dans les établissements pénitentiaires genevois.

II. Le Préposé cantonal à la protection des données et à la transparence observe en droit:

6. 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) ou encore le droit d'être protégé contre l'emploi abusif des données personnelles (art. 13 al. 2 Cst.).
7. 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.
8. 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 (arrêt du Tribunal fédéral 4A_576/2015, du 29 mars 2016, consid. 2.2.1).
9. Entrée en vigueur le 1^{er} mars 2002, la LIPAD pose le principe de la transparence des institutions publiques. Son but est de favoriser la libre formation de l'opinion et la participation à la vie publique des citoyennes et des citoyens. A ce titre, la loi leur donne des droits en matière d'accès aux documents en lien avec les activités des institutions publiques.
10. En 2008, la loi a fait l'objet d'une révision importante: la protection des données personnelles a été ajoutée au volet transparence. De la sorte, un autre objectif figure désormais dans le texte: protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant.
11. La LIPAD est applicable aux institutions publiques genevoises, en particulier aux "pouvoirs exécutif, législatif et judiciaire cantonaux, ainsi que leurs administrations et les commissions qui en dépendent" (art. 3 al. 1 litt. a LIPAD). Le Département de la sécurité, de la population et de la santé (DSPP) est l'un des sept départements de l'administration cantonale (art. 1 al. 1 litt. c du règlement sur l'organisation de l'administration cantonale du 1er juin 2018; ROAC; RSGe B 4 05.10). De la sorte, la LIPAD lui est applicable (art. 3 al. 1 litt. a).
12. 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). Tant que les données n'ont pas été rendues anonymes, l'on se trouve face à des questions relatives à la protection de données personnelles.
13. Les données personnelles sensibles comprennent 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).

14. La loi énonce un certain nombre de principes généraux régissant la protection des données personnelles (art. 35 à 40 LIPAD), soit en particulier:

– **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, la loi stipule que 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.

– **Bonne foi** (art. 38 LIPAD)

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. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

– **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.

15. La LIPAD prévoit des règles spécifiques relatives à la vidéosurveillance à son art. 42:

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.

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

17. L'art. 8 de la loi sur l'organisation des établissements et le statut du personnel pénitentiaires du 3 novembre 2016 (LOPP; RSGe F 1 50) 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.

18. 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".*

19. Les art. 21 à 23 ROPP (Règlement sur l'organisation des établissements et le statut du personnel pénitentiaires du 22 février 2017; RSGe F 1 50.01) 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.

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

21. L'art. 47 LIPAD détermine les prétentions que toute personne physique ou morale de droit privé peut exiger des institutions publiques à propos des données la concernant, soit qu'elles s'abstiennent de procéder à un traitement illicite, le cas échéant qu'elles

mettent fin à un tel traitement et en suppriment les effets, ou qu'elles constatent le caractère illicite de ce traitement, qu'elles détruisent celles qui ne sont pas pertinentes ou nécessaires (sauf disposition légale contraire), rectifient, complètent ou mettent à jour celles qui sont respectivement inexactes, incomplètes ou dépassées, ou fassent figurer, en regard de celles dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées, une mention appropriée, à transmettre également lors de leur communication éventuelle. L'exposé des motifs accompagnant le projet de loi spécifie que "*seule une personne physique ou morale de droit privé se voit conférer des droits en relation avec ses propres données personnelles*" (MGC 2005-2006 X A 8516).

22. A l'instar de ce que prévoit le droit fédéral, a ainsi qualité pour agir au sens de la disposition précitée la personne physique ou morale, victime d'une atteinte illicite à sa personnalité par le traitement entrepris sur les données la concernant (Meier Philippe, Protection des données, fondements, principes généraux et droit privé, Berne 2011, p. 585).
23. L'art. 7 LPA prévoit ce qui suit: "*Ont qualité de partie les personnes dont les droits ou les obligations pourraient être touchés par la décision à prendre, ainsi que les autres personnes, organisations ou autorités qui disposent d'un moyen de droit contre cette décision*". Selon l'art. 60 al. 1 LPA, "*ont qualité pour recourir: a) les parties à la procédure qui a abouti à la décision attaquée; b) toute personne qui est touchée directement par une loi constitutionnelle, une loi, un règlement du Conseil d'Etat ou une décision et a un intérêt personnel digne de protection à ce que l'acte soit annulé ou modifié*".
24. Dans un arrêt du 15 octobre 2019 (ATA/1520/2019), la Cour de justice a rappelé que les let. a et b de la disposition précitée devaient se lire en parallèle, de sorte qu'un intérêt digne de protection devait être présent. L'intérêt digne de protection doit être actuel et concret, dans un rapport suffisamment étroit, spécial et digne d'être pris en considération; le recours d'un particulier formé dans l'intérêt général ou dans l'intérêt d'un tiers est exclu. S'agissant d'une association, elle "*a qualité pour recourir à titre personnel lorsqu'elle remplit les conditions posées à l'art. 89 al. 1 LTF. En outre, sans être elle-même touchée par la décision entreprise, une association peut être admise à agir par la voie du recours en matière de droit public - recours dit corporatif ou égoïste - pour autant qu'elle ait pour but statutaire la défense des intérêts de ses membres, que ces intérêts soient communs à la majorité ou au moins à un grand nombre d'entre eux et, enfin, que chacun de ceux-ci ait qualité pour s'en prévaloir à titre individuel. En revanche, elle ne peut prendre fait et cause pour l'un de ses membres ou pour une minorité d'entre eux (ATF 137 II 40 consid. 2.6.4 et les arrêts cités). Lorsque l'acte attaqué est un acte normatif, l'intérêt personnel requis peut être simplement virtuel; il suffit qu'il existe un minimum de vraisemblance que le recourant puisse se voir un jour appliquer les dispositions contestées (ATF 136 I 49 consid. 2.1; 130 I 26 consid. 1.2.1 et la jurisprudence citée)*".
25. Selon l'art. 49 al. 1 LIPAD, toute requête fondée sur les art. 44, 47 ou 48 doit être adressée par écrit au responsable en charge de la surveillance de l'organe dont relève le traitement considéré. Selon l'exposé des motifs accompagnant le projet de loi, la phase non contentieuse débute donc par une "*requête formelle à adresser par écrit*" (MGC 2005-2006 X A 8520).
26. Conformément à l'art. 18A LPA, la communication électronique entre les parties, les tiers et les autorités est admise (al. 1) selon les formats fixés par le Conseil d'Etat par voie réglementaire (al. 4) pour autant qu'elle respecte les principes de la sécurité des communications, de la coordination avec les normes édictées par la Confédération et de la protection de la bonne foi (al. 2). Lorsqu'elle est utilisée, les exigences de la forme écrite et de la signature manuscrite posées par le droit cantonal ne s'appliquent pas (al.

5). Selon l'exposé des motifs relatif à cette disposition, "*Comme il ne suffit pas de prévoir l'autorisation de communiquer électroniquement (al. 1), il faut encore régler la question des exigences de « forme écrite », de « signature », de « signature manuscrite » prévues dans des lois spéciales ou des règlements. L'alinéa 3¹ prévoit le principe d'équivalence: lorsqu'elle est admise et utilisée, la communication électronique suffit et remplace la forme écrite et la signature manuscrite*" (MGC 2008-2009/X A 13502).

27. Le Règlement sur l'administration en ligne du 26 juin 2019 (RAeL; RSGe B 4 23.01) contient notamment les dispositions d'exécution de la LPA concernant la communication électronique en matière non contentieuse (art. 1 al. 1 RAeL). Son art. 4 prévoit les canaux numériques de communication dans les relations avec les administrés, dont le courrier électronique (let. a). L'art. 5 régit la question du choix du canal numérique de communication et dispose à son al. 1 que l'office concerné, d'entente avec l'office cantonal des systèmes d'information et du numérique, détermine le canal numérique de communication suite à une analyse de risques (al. 3 et 4).
28. Une institution publique qui n'entend pas donner suite à une prétention fondée sur les art. 44, 47 ou 48 LIPAD doit transmettre la requête au Préposé cantonal avec ses observations, afin qu'il rende une recommandation écrite à son attention et à celle du requérant (art. 49 al. 4 et 5 LIPAD).

III. Le Préposé cantonal à la protection des données et à la transparence considère:

29. Le Préposé cantonal relève que, outre la question de fond, deux questions liées à la recevabilité de la requête lui sont soumises par la responsable LIPAD du DSPPS. Il convient de les examiner au préalable.
30. La première a trait à la forme de la requête, l'art. 49 LIPAD exigeant que cette dernière soit adressée au responsable LIPAD "par écrit". Or, la requête donnant lieu à la présente recommandation a été formulée par courriel. Les Préposés observent que l'art. 18A LPA constitue une base légale pour la communication électronique entre une partie et l'autorité, forme de communication qui, si elle est admise, suffit et remplace la forme écrite et la signature manuscrite (art. 18A al. 5 LPA). Les conditions d'utilisation de la communication électronique sont au surplus régies par règlement dont il ressort que le choix du canal est déterminé par l'office concerné (art. 5 al. 3 – 4 RAeL). Le DSPPS a donc une certaine latitude quant au choix du canal de communication.
31. En l'espèce, la requête est intervenue par courriel le 9 décembre 2022. Depuis cette date, soit plus de 4 mois à ce jour, le DSPPS n'a pas demandé à Me X de lui adresser sa demande sous une autre forme, soit par écrit avec signature manuscrite. De plus, à la connaissance des Préposés et au vu du contexte entourant le dossier, il ne semble pas qu'il y ait un doute sur l'authenticité de la demande. Dès lors, pour eux, ce serait faire preuve d'un très grand formalisme que d'exiger de Me X qu'il formule sa demande par un autre canal de communication. Cela étant, ce qui précède n'implique pas que l'ensemble de la procédure puisse se dérouler par ce canal de communication (notification de la décision notamment).
32. La deuxième question soumise au Préposé cantonal a trait à la qualité pour agir des requérants, à savoir M. B d'une part, et A d'autre part. Les décisions sollicitées par les requérants se fondent sur l'art. 47 LIPAD, disposition qui peut être invoquée par toute victime d'une atteinte illicite à sa personnalité par le traitement entrepris sur les données la concernant. Les Préposés considèrent que, selon cette disposition, seule une personne effectivement touchée par l'utilisation des "bodycams" a qualité pour agir – la

¹ L'actuel al. 5 de l'art. 18A était initialement son al. 3.

question de la qualité pour agir des associations sera abordée ci-dessous –. Dès lors, si une personne n'est jamais amenée à être filmée par les "bodycams", ni même à les utiliser, l'on ne voit pas en quoi elle serait touchée de manière directe, concrète et dans une mesure et avec une intensité plus grande que les autres administrés. Sa qualité pour agir ferait défaut. En l'espèce, sur la base du cahier des charges relatif à la fonction de M. B qui a été remis aux Préposés, il leur est impossible de conclure qu'un tel usage soit absolument exclu dans sa fonction. Ils recommandent donc à la responsable du DSPS de vérifier ce point en pratique et de permettre au requérant de s'exprimer à cet égard. S'il devait s'avérer que le requérant n'a pas la qualité pour agir, il ne saurait être donné une suite positive à sa requête.

33. S'agissant de A, les Préposés considèrent qu'elle n'a pas qualité pour agir à titre personnel, faute d'être elle-même lésée par l'utilisation des bodycams. Se pose la question de sa qualité pour agir à titre corporatif. Les Préposés considèrent que ce que la Cour de justice a retenu dans son arrêt du 15 octobre 2019 (ATA/1520/2019) portant précisément sur la qualité pour agir de A dans une situation concernant uniquement les agents de détentions, peut s'appliquer *mutatis mutandis*. Ainsi, A doit démontrer que les intérêts d'une majorité de ses membres sont touchés, ou que chacun des membres a, à titre individuel, qualité pour agir. En l'espèce, il semblerait douteux que la majorité des membres ait à titre individuel qualité pour agir, ou que les intérêts d'une grande majorité des membres de A soient touchés, puisque le syndicat représente certes les intérêts des agents de détention mais aussi ceux des policiers, inspecteurs de l'office cantonal des véhicules, ainsi que ceux des retraités des catégories précitées, pour qui l'utilisation des bodycams dans les prisons n'a aucune répercussion. Les Préposés partagent ici le point de vue de la responsable LIPAD.
34. Sur le fond, concernant l'utilisation de bodycams dans les prisons, les Préposés avaient exposé ce qui suit dans leur avis du 10 octobre 2022: *"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"*.
35. Les Préposés avaient ensuite souligné que les problématiques les plus saillantes avaient trait d'une part au fait que des fouilles de personnes détenues pouvaient être filmées, et d'autre part à la question de la reconnaissabilité de l'utilisation de la caméra, ainsi que de

la communication faite aux personnes concernées, notant qu'un enregistrement à l'insu de la personne concernée devrait être expressément interdit.

36. Il en découle que la problématique de l'absence de base légale et du besoin d'un encadrement plus adéquat du dispositif d'utilisation des bodycams relevait principalement de la protection de la personnalité des détenus. En effet, ces derniers n'ont aucun contrôle sur la mise en œuvre du dispositif, ni sur le début ou la fin d'un enregistrement.
37. C'est dans cette optique que les Préposés avaient suggéré l'adoption de bases légales idoines et la consultation des représentants de toutes les parties concernées en vue de l'élaboration d'un projet de loi. Ils relèvent que des démarches dans ce sens ont d'ores et déjà été entreprises par le DSPS.

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande au Département de la sécurité, de la population et de la santé:

- d'examiner la qualité pour agir de M. B et, si besoin, de lui octroyer un délai pour se déterminer sur ce point.
- de finaliser un projet de base légale concernant l'utilisation de bodycams dans les prisons.

La présente recommandation est notifiée par pli recommandé à:

- Me X
- Mme Hana Sultan Warnier, responsable LIPAD, Département de la sécurité, de la population et de la santé, Secrétariat général, Direction juridique, rue de l'Hôtel-de-Ville 14, Case postale 3952, 1211 Genève 3

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal