Projet de loi sur l'information de police (LIPol)

Avis du 25 août 2022

Mots clés: veille législative, base légale, données personnelles, données personnelles sensibles, informations de police, profilage, enregistrements audio et vidéo, lecture automatiques de plaques, contrôles préventifs, communication de données, destruction des données.

Contexte: Le 29 juillet 2022, la Chancellerie d'Etat (CHA) a requis l'avis du Préposé cantonal à la protection des données et à la transparence (ci-après le Préposé cantonal) au sujet d'un projet de loi sur l'information de police (LIPol). L'ensemble du projet de loi a trait à des questions de protection des données personnelles.

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

1. Caractéristiques de la demande

Par courriel du 29 juillet 2022, la Chancellerie d'Etat (CHA) a requis l'avis du Préposé cantonal à la protection des données et à la transparence (ci-après le Préposé cantonal) au sujet d'un projet de loi sur l'information de police (LIPol). L'avis du Préposé cantonal est souhaité pour le 30 septembre 2022. De par son objet, l'ensemble du projet a trait à des questions de protection des données personnelles.

Selon l'exposé des motifs accompagnant ledit projet, il s'est agi de s'orienter vers une refonte complète de la loi sur les renseignements et les dossiers de police et la délivrance des certificats de bonne vie et mœurs, du 29 septembre 1977 (LCBVM; RSGe F 1 25), de positionner l'information comme thème central de la nouvelle loi et de rédiger le projet de loi en suivant le cycle de vie de l'information: *"La police constitue l'information par la collecte de données de toutes sortes, ensuite elle la protège par la mise en place de mesures techniques et organisationnelles adéquates, puis elle y accède pour travailler avec, l'enrichir et/ou la mettre à jour, ou encore pour la communiquer à des institutions publiques ou à des privés selon les dispositions légales, et, enfin lorsque certaines conditions sont remplies, l'information arrive en fin de vie et doit être détruite, ou anonymisée ou encore archivée. Ce projet de loi permet d'avancer de manière significative dans la création de bases légales spécifiques pour les activités de la police en matière de collecte et de traitement de l'information*".

L'exposé des motifs définit encore les objectifs de la nouvelle loi comme suit:

- "*régir tout le cycle de vie de l'information de police (constitution, protection, communication et diffusion, modification, destruction ou archivage);*

- *distinguer l'information de police de toute autre information qui ne serait pas de police, quand bien même celle-ci serait utilisée à la police ou par la police;*

- *prendre en charge correctement les besoins opérationnels de la police, en matière de traitement de l'information;*

- *reprendre et reformuler au besoin certaines dispositions encore utiles de la LCBVM;*

- *prendre en compte les véritables enjeux actuels et se débarrasser de certains legs sociologiques ou historiques devenus peu pertinents voire inutiles (par ex. certificat de bonne vie et mœurs);*

- *offrir au commandant de la police les moyens juridiques d'assurer le contrôle de l'utilisation des données de police par ses collaborateurs;*

- *permettre une meilleure mise en cohérence avec les exigences de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (ci-après: LIPAD) en matière de protection des données et les obligations de la police*".

Seules les dispositions qui appellent des commentaires seront ici reprises, puis commentées dans l'appréciation au point 3 ci-dessous.

Art. 3 Définitions

Dans la présente loi et ses règlements d'application, on entend par:
a) données de police, tout élément d'information recueilli par la police cantonale et la police municipale dans le cadre de leurs missions, quelle que soit sa source;
b) information de police, l'ensemble des données de police collectées et conservées sous forme de fichiers;
c) dossier de police, l'ensemble des informations de police relatives à une personne identifiée, collectées et conservées dans le cadre des activités de police judiciaire au sens de l'article 10A de la loi d'application du code pénal suisse et d'autres lois fédérales en matière pénale, du 27 août 2009. Ce dossier est unique et est conservé par la police cantonale.

Art. 4 Collecte de données

[1] La police collecte et exploite toutes les données nécessaires à l'accomplissement de ses tâches légales.
[2] Les organes qui exercent sur le territoire du canton de Genève des compétences judiciaires au sens de l'article 10A LaCP remettent à la police cantonale une copie des rapports qu'ils dressent.

Art. 5 Données personnelles sensibles et profilage

[1] La police cantonale et la police municipale collectent et exploitent des données personnelles sensibles et établissent des profilages:
a) à des fins de prévention des crimes et délits;
b) lorsque la poursuite et la répression des infractions le rendent nécessaire;
c) pour assurer la sécurité des personnes et des biens.
[2] La police peut collecter et exploiter des données personnelles sensibles et établir des profilages:
a) dans les processus de recrutement de son personnel;
b) dans le cadre des procédures d'accréditation du personnel d'autres services de l'Etat et d'entreprises mandatées par l'Etat.
[3] Les données collectées en application de l'alinéa 2 sont détruites:
a) à l'expiration de la période probatoire, pour les personnes engagées;
b) à l'issue de la durée de validité de l'accréditation;
c) immédiatement en cas de non engagement ou de refus de l'accréditation.

L'exposé des motifs précise au sujet de cette disposition que "*hormis les cas usuels où la police a besoin de traiter des données personnelles sensibles (lettres a, b et c) et actuellement prévus par la LCBVM, il est apparu nécessaire de doter de bases légales des situations où la police doit traiter des données personnelles sensibles en dehors d'une activité de police proprement dite. Tel est le but de l'alinéa 2 qui dote la police d'une base légale pour mettre en œuvre des procédures de contrôles de sécurité sur des personnes, soit dans le cadre des processus de recrutement de son personnel interne, soit dans le cadre du recrutement de leur personnel interne par d'autres services de l'Etat, soit enfin dans le cadre des*

accréditations de personnels externes mandatés par la police ou par un autre service de l'Etat pour travailler sur des biens, dans les locaux ou au nom et pour le compte de la police. Cette disposition répond par ailleurs de manière adéquate à la suppression du certificat de bonne vie et mœurs et, pour cette raison, s'applique à ce qui est communément appelé le "Grand Etat" à savoir le Petit Etat constitué des sept départements, de la chancellerie, du Pouvoir judiciaire et du service du Grand Conseil, auquel s'additionnent les établissements publics autonomes et d'autres entités sis dans le canton et qui fournissent des prestations de caractère public, généralement en référence à des lois cantonales". Les exemples relatifs à cette disposition ont trait au personnel de nettoyage dans les locaux de la police, de techniciens chargés de déployer des systèmes d'information ou encore les entreprises d'enlèvement de véhicules en cas d'accident. Il est encore précisé que cette disposition s'inspire de ce que prévoit la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, du 21 mars 1997 (LMSI; RS 120) ou encore les dispositions cantonales bernoises de la loi sur la police du canton de Berne, du 10 février 2019 (Lpol; RSB 551.1) organisant et fixant les conditions du contrôle de sécurité relatif aux personnes. Toutefois, l'exposé de motifs précise encore ce qui suit: "*Contrairement à la législation bernoise qui a réglé les modalités de mise en œuvre des contrôles de sécurité dans la loi, l'option faite dans ce projet de loi est de fixer le principe dans la loi et de régir les modalités pratiques dans le règlement d'application*".

Il est finalement indiqué que les délais de conservation ont été fixés pour concilier à la fois les besoins opérationnels de la police en terme de contrôles de sécurité et les principes de la protection des données personnelles, notamment les principes de proportionnalité et de minimisation des atteintes.

Art. 6 Données collectées lors d'interventions de police

[1] Sans préjudice de l'exercice de la vidéosurveillance de leurs locaux en application de l'article 61 de la loi sur la police, du 9 septembre 2014, et de l'article 12A 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, la police cantonale et la police municipale peuvent, à des fins de preuve et de prévention, photographier ou filmer leurs interventions.

[2] A cet effet, elles peuvent équiper leurs agents et leurs véhicules de systèmes de collecte de données audiovisuelles.

[3] Les données sont conservées pendant 100 jours avant d'être détruites, sauf décision contraire d'une autorité compétente.

Selon l'exposé des motifs, les deux premiers alinéas autorisent notamment l'utilisation de caméras-piétons, de drones et de caméras embarquées dans les véhicules de police et dans ceux utilisés par les membres de la police municipale.

Il est également indiqué que "*l'intérêt pratique de cet article est que, d'une part, il ne crée pas d'obligation mais offre à la police et à la police municipale la faculté d'utiliser ces dispositifs le jour où la nécessité l'exigera et les moyens le permettront et que, d'autre part, il est technologiquement neutre, ce qui permet de s'adapter aux évolutions technologiques sans modifier la loi.*

Enfin, il est à préciser qu'en principe, les données ainsi collectées ne sont pas systématiquement exploitées. Elles ne sont consultées et exploitées qu'en cas de besoin, notamment à des fins de preuve, et sur décision d'une autorité compétente.

Les données ainsi collectées sont conservées pendant 100 jours afin de s'assurer de leur disponibilité en cas de dépôt de plainte dans le délai légal. Cas échéant, ces données sont gardées le temps de la procédure. L'article 9 ci-dessous prévoit l'utilisation des données à des fins de formation, de conduites opérationnelles, à la condition qu'il n'y ait pas de procédure pénale pendante et que la personnalité des personnes figurant de manière reconnaissable dans ces données soit préservée".

Art. 7 Lecture automatique de plaques d'immatriculation

[1] La police et la police municipale peuvent recourir à des dispositifs de lecture automatique et de reconnaissance de plaques d'immatriculation.

[2] Les données collectées sont conservées pendant 100 jours avant d'être détruites, sauf décision contraire d'une autorité compétente.

Il est explicité dans l'exposé des motifs qu'il s'agit, avec cette disposition, d'ancrer dans la loi genevoise l'utilisation par la police cantonale de dispositifs de lecture automatique de plaques d'immatriculation pour optimiser ses tâches notamment en matière de sécurité routière. De plus, cette disposition étend par ailleurs à la police municipale la possibilité d'exploiter ce type de dispositif.

S'agissant des finalités de l'utilisation, il est indiqué ce qui suit: "*un tel dispositif peut permettre de repérer des plaques d'immatriculation de véhicules étrangers recherchés en Suisse pour des contraventions (amendes non payées), mais il peut également être utilisé lors de recherches de véhicules volés ou impliqués dans des évènements ou faits graves (accident mortel), ou inquiétants (recherche de personne disparue, kidnapping d'enfant), etc*".

Art. 8 Enregistrement des appels téléphoniques et des communications radio

[1] La police cantonale et la police municipale enregistrent, à des fins de preuve, de formation, ou de contrôle qualité:

a) les appels entrants et sortants gérés par leurs centrales téléphoniques;
b) les communications radio, selon les options techniques disponibles et leurs évolutions;
c) les appels émis depuis un numéro externe et reçus sur les numéros généraux des postes et brigades, moyennant la diffusion d'un message d'avertissement.

[2] Les données sont conservées pendant 12 mois et sont détruites à l'expiration de ce délai de conservation, sauf décision contraire d'une autorité compétente.

Selon l'exposé de motifs, "*cette nouvelle disposition permet d'asseoir l'enregistrement des conversations téléphoniques et radio sur une base légale formelle qui fixe clairement les finalités précises pour lesquelles l'enregistrement est autorisé et qui prévoit également la durée de conservation des données ainsi enregistrées*". Il est ajouté que conformément au principe de la reconnaissabilité (bonne foi) de toute collecte de données personnelles, une annonce doit indiquer à l'interlocuteur externe que la conversation avec les services de police sera enregistrée.

Art. 9 Utilisation des données audio et audiovisuelles à des fins de conduite, de formation et d'information

[1] La police peut utiliser des données collectées en vertu des articles 6, 7 et 8 à des fins de conduite, de formation et d'information.

[2] Des mesures organisationnelles et des procédés techniques d'anonymisation sont appliqués pour préserver, si nécessaire, la personnalité des personnes concernées.

L'exposé des motifs précise ce qui suit: "*Cette nouvelle disposition permet une utilisation des données collectées à des fins de conduite opérationnelle mais également de formation et d'information. Cette utilisation des données est indispensable à la réalisation de retours d'expériences (RETEX) suite à des opérations de police particulières, inédites ou de grande ampleur, nécessitant une évaluation de l'ensemble des processus mis en œuvre à des fins d'amélioration continue et de perfectionnement de la conduite des opérations par les chefs d'engagements. Ces données sont également nécessaires à la formation des collaborateurs de la police à travers l'analyse de cas pratiques. Enfin dans le cadre notamment de son obligation de communiquer spontanément au public les informations qui sont de nature à*

l'intéresser (article 18 LIPAD), la police peut être amenée à devoir utiliser ces données audio et audiovisuelles. Il s'agit par exemple d'illustrer certains modes opératoires dans le cadre de campagnes de prévention.

L'utilisation de ces données n'est toutefois admissible que dans la mesure où aucune loi (code de procédure pénale par exemple) ni aucun règlement, ni aucune décision d'une autorité compétente ne l'interdit ou qu'un intérêt public ou privé prépondérant ne s'y oppose.

L'alinéa 2 précise les conditions à remplir pour éviter toute atteinte non nécessaire et non justifiée à la personnalité des personnes dont les données ont été collectées".

Art. 13 Contrôles préventifs nominatifs

[1] Sur ordre du commandant, l'utilisation des systèmes d'information peut faire l'objet de contrôles préventifs nominatifs.

[2] L'utilisateur concerné est informé du contrôle. À sa demande, il en reçoit le résultat.

[3] Si l'utilisateur ayant fait l'objet du contrôle ne fait pas partie de la police cantonale, le commandant transmet le résultat du contrôle à son chef de corps de police municipale qui prend les mesures adéquates et en donne quittance au commandant.

L'exposé des motifs indique: "*S'agissant de l'article 13, son alinéa 1 constitue une nouveauté car il permet, en l'absence de tout indice d'abus, de compromission ou de risque identifiés, de procéder à des contrôles préventifs de l'utilisation des ressources par un ou plusieurs collaborateurs.*

Le commandant peut désigner une catégorie de collaborateurs (ex. tous les collaborateurs ayant accès à une base de données spécifiques ou ayant une fonction spécifique) ou un service spécifique (par exemple un service sensible ou disposant d'accès privilégiés) et ordonner que leur utilisation de tout ou partie des systèmes d'information soit contrôlée, soit demander que l'utilisation d'un fichier ou d'une base de données soit contrôlée de manière ciblée. Dans les deux cas, les noms des collaborateurs seront visibles lors du contrôle et aucun indice laissant croire à la vraisemblance d'un risque n'aura été préalablement nécessaire avant de lancer le contrôle.

Ces contrôles ont un but pédagogique et dissuasif, car ils permettent de rappeler aux membres de la police cantonale et de la police municipale qu'ils peuvent en tout temps être appelés à rendre compte de l'utilisation qu'ils font des ressources informationnelles mises à leur disposition pour accomplir leurs tâches. En termes de gestion des risques et de la qualité, il est à relever que les bons résultats des contrôles constitueront des indicateurs permettant d'attester du traitement correct des données de la police et de la police municipale par leurs collaborateurs.

Dans la mise en œuvre pratique en interne police, il revient au commandant de dresser la liste des fichiers ou ressources informatiques qu'il estime concernés par ces contrôles car cette liste doit être évolutive pour s'adapter aux moyens, aux enjeux et aux risques sur l'information de police. Mais, dans tous les cas, il s'agira de fichiers cantonaux ou fédéraux qui contiennent des informations de nature purement policière et dont l'accès et la consultation sont strictement limités aux besoins opérationnels. A titre d'exemple on peut citer ABI Affaires, myABI Journal, CALVIN, certains espaces de stockage de photos d'accidents graves de circulation, d'images de vidéosurveillance, etc.

A noter que le collaborateur est informé des contrôles et dispose du droit d'accès aux résultats.

En fonction des constatations effectuées lors du contrôle ciblé, le commandant prend les mesures disciplinaires adéquates et/ou, cas échéant, dénonce les faits constitutifs d'infraction pénale au Procureur général, conformément aux articles 64 LIPAD, 23A RPAC et 323 Code pénal."

Art. 16 Droits de la personne concernée

[4] Lorsque la requête porte sur le journal des évènements de la police, la communication des informations est faite sous la forme d'un rapport d'information sommaire qui ne peut contenir que les informations que la police a pu vérifier ou qu'elle a constatées elle-même, à l'exclusion des simples déclarations qui lui ont été faites. Le commandant fixe, par voie de directive, le contenu de ce rapport d'information.

Quant à cette disposition, l'exposé des motifs relève qu'elle "*s'intéresse à l'épineuse question du droit d'accès aux données contenues dans le journal des évènements de la police et propose de nouvelles règles pour cadrer le contenu et le format des données à communiquer. Il sied de signaler que, dès le début de la refonte de la LCBVM, un accent particulier a été mis sur les conditions d'accès au journal des évènements de la police dans le cadre du droit d'accès à ses données personnelles. Il convient de rappeler que le journal des évènements par ailleurs appelé, improprement, "mains courantes de la police" est la forme informatisée des registres de main courante ou des calepins sur lesquels les agents de police consignaient au fur et à mesure leurs constatations effectuées sur le terrain, de manière brute, en l'état. C'est avec la mise en place du système d'information central de la police P2K à la fin 2003 que le journal des évènements a été mis en production pour contenir l'ensemble des réquisitions de la police ayant fait l'objet d'une inscription et les constatations faites sur place par les agents de police.*

Le journal des évènements de police contient donc des informations brutes, souvent non vérifiées, non complétées et jamais mises à jour car correspondant aux constatations matérielles des agents et aux déclarations des parties et témoins au moment de l'événement. Ces informations sont volontairement conservées à l'état brut. Les évolutions de la situation et les informations provenant d'actes d'enquête font l'objet de documents subséquents. Par conséquent, la valeur probante des informations de ce journal est toute relative tant que les faits qu'elles concernent n'auront pas été établis par décision de justice devenue définitive.

Cependant, de plus en plus de citoyens, soit directement soit via leur avocat, demandent, en invoquant leur droit d'accès à leurs données personnelles, à accéder à des extraits de ce journal des évènements à des fins diverses et variées, mais souvent judiciaires, parfois éloignées des objectifs et de la nature de ce journal. Les informations contenues dans ces extraits peuvent engendrer le doute plutôt que de contribuer à l'élucidation d'une affaire ou la clarification des circonstances d'un événement. Cela est d'autant plus probable lorsque la suite d'une affaire prend une tournure différente des informations brutes originelles.

C'est pour cette raison qu'il est apparu nécessaire de prévoir dans la nouvelle loi une disposition visant à fixer de manière précise les informations du journal des interventions de police que la police est habilitée à fournir dans le cadre de l'exercice du droit d'accès aux données personnelles prévu par l'article 44 LIPAD. Le nouveau cadre est fixé par le nouvel article 16 alinéa 4 qui dispose que lorsque "la requête porte sur le journal des évènements de la police, la communication des informations est faite sous la forme d'un rapport d'information sommaire qui ne peut contenir que les informations que la police a pu vérifier ou qu'elle a constatées elle-même, à l'exclusion des simples déclarations faites à la police." Cette solution permet de garantir l'exercice du droit d'accès à ses données personnelles tout en évitant que des informations non vérifiées ou fausses soient colportées voire utilisées à des fins ne correspondant pas aux finalités pour lesquelles elles ont été collectées. Pour le surplus, il est confié au commandant la charge de fixer, par voie de directive, le contenu de ce rapport d'information".

Chapitre IV Communication d'informations de police à des institutions publiques

Art. 19 En vertu d'une base légale

La police, d'office ou sur requête, transmet, par écrit, aux institutions cantonales ou fédérales autorisées par une base légale fédérale ou cantonale à les recevoir, les informations nécessaires à l'accomplissement de leurs tâches légales.

Art. 20 Sur requête

La police est autorisée à communiquer, par écrit et sur requête motivée, à d'autres autorités les données nécessaires à l'exécution des tâches qui leur sont confiées par la loi, pour autant qu'aucun intérêt privé ou public prépondérant ne s'y oppose.

Sur la distinction entre les art. 19 et 20 du projet, l'exposé des motifs note que l'article 19 concerne les institutions qui disposent dans une autre loi, d'une autorisation légale ou base légale qui leur permet de demander des informations de police, alors que l'art. 20 concerne toutes les autres institutions qui ne disposent pas de base légale leur permettant d'obtenir obligatoirement des informations de police. Cette dernière disposition autorise la police à recevoir et traiter leur demande et leur fournir les informations de police pour autant qu'aucun intérêt privé ou public prépondérant ne s'y oppose.

L'exposé des motifs liste en outre les bases légales existantes permettant une communication de données au sens de l'art. 19 du projet de loi.

Cette disposition se veut la base légale formelle pour la transmission d'informations de police à différentes administrations "*dans le but de leur permettre d'effectuer une appréciation complète, par exemple, du dossier d'un candidat à un poste dans l'administration cantonale, au pouvoir judiciaire ou des établissements de droit public (par exemple l'AIG, les SIG, les TPG) ou encore, s'agissant d'un prestataire de service devant œuvrer dans les locaux de ces administrations ou établissements de droit public. En effet, il serait regrettable de laisser des personnes reconnues coupables d'une escroquerie ou d'une infraction grave accéder à certaines fonctions sensibles au sein de l'Etat ou de laisser des personnes déjà condamnées pour vol de bien matériel ou de données informatiques accéder à certains locaux de l'Etat. De même, il est dans l'intérêt de la police et de l'Etat qu'un office comme l'office cantonal des systèmes d'information et du numérique puisse évaluer de manière exhaustive les candidatures des personnes destinées à travailler sur des données sensibles de la police ou de l'administration cantonale en général. Dès lors, la transmission d'informations non soumises au secret de procédure à des entités ou personnes spécifiques en vue de procéder à des contrôles de sécurité dans le cadre d'un engagement ou d'une accréditation semble être dictée par le devoir, voire l'obligation, de partager des informations nécessaires à la réalisation des missions d'intérêt général*".

Toujours concernant l'art. 20 du projet, il est indiqué que "*dans cet article également, l'option est faite de ne pas lister les institutions autorisées à recevoir des informations de police sur requête; ce qui correspond à un changement de paradigme dans la mesure où désormais, au lieu de quelques institutions listées, c'est toutes les institutions publiques qui peuvent demander des informations de police et le seul filtre ou frein est une injonction légale ou une décision contraire ou la présence d'intérêt privé ou public prépondérant qui s'opposerait à la communication des informations. Cette approche pragmatique se justifie d'autant plus qu'il est proposé dans ce projet de loi de ne plus délivrer de certificat de bonne vie et mœurs*".

Art. 21 Destruction d'office

[1] Sous réserve des dispositions de la loi sur les archives publiques (ci-après LArch), du 1er décembre 2000, la police procède à la destruction des informations contenues dans le dossier de police à l'expiration de la durée de conservation. Cette dernière est déterminée, pour chaque dossier par l'infraction la plus grave ou par l'infraction la plus récente, réalisée ou non.

[2] Pour déterminer la durée de conservation des informations contenues dans le dossier, il est tenu compte des délais suivants:

a) après 99 ans en cas de crimes imprescriptibles (article 101 alinéa 1 du Code pénal);

b) après 50 ans pour les infractions graves;

c) après 30 ans pour les infractions ne relevant pas des lettres a, b et d);

d) après 10 ans s'il s'agit d'une contravention.

En cas de nouveau crime ou délit, le délai sera recalculé pour conserver l'ensemble du dossier.

[3] Le commandant édicte, après consultation du procureur général, les critères de classification des infractions graves et les règles de computation.

[4] Les données du journal des évènements, non liées à des catégories d'infractions susmentionnées, sont conservées pendant 10 ans à compter de la date de leur enregistrement.

L'exposé des motifs précise que cette disposition vise la destruction automatique des données. L'art. 22 réserve la possibilité d'une destruction anticipée des données, sur demande de la personne concernée.

2. Les dispositions légales pertinentes

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) a fait l'objet d'une révision importante en 2008, par laquelle la protection des données personnelles a été ajoutée au champ d'application matériel de la loi en sus de son volet relatif à la transparence.

Depuis le 1er janvier 2010, date de l'entrée en vigueur de cette modification législative, un autre objectif figure désormais dans le texte légal à son art. 1 al. 2 litt. b: "*protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant*".

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, la loi vise 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).

La LIPAD énonce un certain nombre de principes généraux régissant la collecte et le traitement des données personnelles (art. 35 à 40 LIPAD).

- Base légale (art. 35 LIPAD)

  Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. Quant aux données personnelles sensibles ou aux profils de la personnalité, ils 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.

L'art. 39 LIPAD traite de la communication de données personnelles selon son destinataire. Les alinéas 1 à 3 ont trait à la communication de données personnelles entre institutions publiques soumises à la LIPAD, les alinéas 4 et 5 à une corporation ou un établissement de droit public suisse non soumis à la loi et les alinéas 6 à 8 à une corporation ou un établissement de droit public étranger.

Cette disposition se lit comme suit:

Art. 39 Communication

A une autre institution publique soumise à la loi

[1] Sans préjudice, le cas échéant, de son devoir de renseigner les instances hiérarchiques supérieures dont elle dépend, une institution publique ne peut communiquer des données personnelles en son sein ou à une autre institution publique que si, cumulativement:

a) l'institution requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait aux exigences prévues aux articles 35 à 38;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[2] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 1 et, une fois la communication effectuée, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement.

[3] Les institutions publiques communiquent aux autorités judiciaires les données personnelles que celles-ci sollicitent aux fins de trancher les causes dont elles sont saisies ou de remplir les tâches de surveillance dont elles sont investies, sauf si le secret de fonction ou un autre secret protégé par la loi s'y oppose.

A une corporation ou un établissement de droit public suisse non soumis à la loi

[4] La communication de données personnelles à une corporation ou un établissement de droit public suisse non soumis à la présente loi n'est possible que si, cumulativement:

a) l'entité requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait à des exigences légales assurant un niveau de protection adéquat de ces données;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[5] L'organe requis est tenu de s'assurer du respect des conditions posées à l'alinéa 4 et, avant de procéder à la communication requise, d'en informer le responsable sous la surveillance duquel il est placé, à moins que le droit de procéder à cette communication ne résulte déjà explicitement d'une loi ou d'un règlement. S'il y a lieu, il assortit la communication de charges et conditions.

A une corporation ou un établissement de droit public étranger

[6] La communication de données personnelles à une corporation ou un établissement de droit public étranger n'est possible que si, cumulativement:

a) l'entité requérante démontre que le traitement qu'elle entend faire des données sollicitées satisfait à des exigences légales assurant un niveau de protection de ces données équivalant aux garanties offertes par la présente loi;

b) la communication des données considérées n'est pas contraire à une loi ou un règlement.

[7] En l'absence du niveau de protection des données requis par l'alinéa précédent, la communication n'est possible que si elle n'est pas contraire à une loi ou un règlement et si, alternativement:

a) elle intervient avec le consentement explicite, libre et éclairé de la personne concernée ou dans son intérêt manifeste;

b) elle est dictée par un intérêt public important manifestement prépondérant reconnu par l'organe requis et que l'entité requérante fournit des garanties fiables suffisantes quant au respect des droits fondamentaux de la personne concernée;

c) le droit fédéral ou un traité international le prévoit.

[8] L'organe requis est tenu de consulter le préposé cantonal avant toute communication. S'il y a lieu, il assortit la communication de charges ou conditions.

Elle est complétée par l'art. 14 RIPAD.

La LIPAD contient une disposition spécifique relative à la vidéosurveillance. Elle prévoit la licéité des systèmes de vidéosurveillance si, cumulativement, la vidéosurveillance est propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proxi-

mité 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; si l'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions; si le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci; et si 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 al. 1 LIPAD).

Les alinéas 2 à 4 précisent les règles concernant la durée de conservation des données, la visualisons des images ou encore leur communication.

3. Appréciation

Le projet de loi présentement soumis aux Préposés a trait au traitement de données personnelles par la police (cantonale et municipale) dans le cadre de ses missions (art. 3 du projet). Dès lors, presque la totalité des dispositions prévues ont un impact en matière de protection des données personnelles. Seules celles appelant des modifications seront commentées dans le présent avis.

Les Préposés ont pris note de la référence à la notion de fichier, notion-clé dans la LIPAD actuelle, pour définir l'information de police. Toutefois, la révision de la LIPAD va mettre l'accent, non plus sur la notion de fichier, ni de maître du fichier, mais sur la notion de traitement des données et de responsable du traitement, à l'instar de la terminologie adoptée par les nouvelles législations (internationale ou suisse) en la matière. Ceci étant précisé, le responsable du traitement correspond à l'actuel maître de fichier, de sorte que les obligations qui lui incombent sont comparables. L'on peut dès lors se demander si **l'art. 3** let b du projet est nécessaire ou si les notions définies aux lettres a) et c) ne seraient pas suffisantes.

L'art. 4 al. 1 du projet constitue une base légale générale à la collecte de données personnelles par la police. Cette disposition pourrait intégrer le principe de proportionnalité de la collecte et se lire comme suit: "La police *peut* collecter et exploiter ~~*toutes*~~ les données *personnelles qui sont strictement* nécessaires à l'accomplissement de ses tâches légales" (les modifications proposées figurent en italique).

Les Préposés relèvent que le projet de loi soumis a notamment pour but de constituer une base légale formelle pour un certain nombre d'activités de la police impliquant le traitement de données personnelles sensibles, voire leur communication.

La conformité des dispositions prévues doit s'examiner au regard des exigences fixées par l'art. 35 al. 2 LIPAD, disposition topique en la matière. Cette dernière dispose 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*". 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" (Grisel Rapin, p. 43[1]). Cette auteure note que 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 rappelle que 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 (Grisel Rapin, p. 48). En l'espèce, le projet de LIPol touche aux droits fondamentaux des citoyens, de sorte que les exigences en matière de densité normative sont élevées.

L'**art. 5** du projet constitue une base légale pour le traitement de données sensibles et le profilage par la police. L'alinéa 1 vise le traitement dans le cadre des activités de police à proprement parler, alors que l'alinéa 2 a trait au traitement de données sensibles par la police hors des activités de police à proprement parler.

S'agissant du premier alinéa, si les finalités de la collecte sont expressément mentionnées, le principe de la proportionnalité pourrait figurer plus clairement dans la formulation de la disposition. En effet, le principe de minimisation des données implique que seules les données strictement nécessaires à une finalité spécifique soient traitées. Ainsi, par exemple, l'art. 5 al. 1 pourrait se lire comme suit: "La police cantonale et la police municipale *peuvent traiter les* données personnelles sensibles *strictement nécessaires*: (…)". En outre, la question du profilage, particulièrement intrusive en matière d'atteinte à la personnalité des personnes concernées, devrait faire l'objet d'un article distinct et voir ses conditions précisées (nécessité d'un soupçon, soupçon portant sur quels types d'infractions, notamment). La densité normative de l'art. 5 à cet égard n'apparaît pas suffisante au regard de l'atteinte portée.

L'art. 5 al. 2 vise le traitement de données personnelles sensibles en dehors d'une activité de police proprement dite. Les Préposés comprennent que la disposition vise à partiellement suppléer à la suppression du certificat de bonne vie et mœurs. S'agissant tout d'abord du profilage, ce qui a été dit ci-dessus peut être repris ici *mutatis mutandis* et une disposition spécifique sur ce point serait souhaitable avec des précisions relatives aux situations dans lesquelles un profilage pourrait intervenir. De plus, il sied de préciser quelle information serait transmise au membre du personnel / candidat concerné et quelle participation de sa part est possible (consentement, participation à l'établissement des faits). En l'espèce, les conditions du profilage n'étant pas précisées, elles pourraient potentiellement intervenir de la même manière pour un membre du personnel que pour une personne sur le point de commettre une infraction (art. 5 al. 1 du projet). Une telle situation n'est évidemment pas souhaitable.

Concernant la formulation de l'art. 5 al. 2, elle apparaît trop peu précise pour que les exigences de l'art. 35 al. 2 LIPAD puissent être considérées comme remplies. D'une part, il sied de rappeler le principe de proportionnalité et de minimisation de la collecte dans la formulation de cette disposition. Idéalement, le type de données sensibles collectées pourrait également être mentionné. D'autre part, la lettre b) de l'art. 5 al. 2 se réfère de manière générale à des procédures d'accréditation. S'il s'agit de procédures d'accréditation prévues par des lois ou règlements, il faudrait le mentionner, car l'exposé des motifs évoque qu'il s'agit de manière générale "*des catégories de personnel qui peuvent, en raison de leur mandat, accéder à des données, des biens et des lieux sensibles*". Une catégorie très large de personnes est ainsi visée. Ainsi, le champ des personnes visées par cette disposition devrait être précisé (soit en se référant simplement au système d'accréditation car il découle de diverses lois ou règlements, soit en précisant les conditions qui font qu'une personne pourrait faire l'objet de tels renseignements). Finalement, l'information transmise aux personnes concernées devrait être clarifiée. S'agissant de l'al. 3, les Préposés saluent le fait que les durées

[1] Clémence Grisel Rapin, La légalité, *in* Bellanger François/Bernard Frédéric, Les grands principes du droit administratif, Zurich 2022.

de conservation des données soient précisées et limitées, ce qui réduit l'atteinte aux personnes concernées.

L'art. 6 du projet permet à la police, à des fins de preuve et de prévention, de photographier ou filmer ses interventions et d'ainsi équiper les agents de caméras. L'exposé des motifs précise que cette disposition autorise l'utilisation de caméras-piétons, de drones et de caméras embarquées dans les véhicules de police et dans ceux utilisés par les membres de la police municipale.

Les Préposés comprennent que cette disposition se veut une base légale à l'utilisation de tels procédés par la police, base légale spéciale par rapport à l'art. 42 LIPAD qui régit la vidéosurveillance de manière générale, en l'absence de base légale spécifique.

Telle que formulée, cette disposition ne fait que mentionner les finalités très larges de l'utilisation de tels dispositifs (à des fins de preuve ou de prévention) sans autres précisions. Il s'agit donc d'un blanc-seing à l'utilisation de telles technologies qui n'est pas compatible avec les exigences de l'art. 42 LIPAD en matière de vidéosurveillance ni avec les principes généraux de protection des données personnelles, en particulier celui de la reconnaissabilité de la collecte[2]. Une base légale autorisant ces pratiques doit les encadrer 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'est à cet égard pas suffisante. En effet, ces prises de vue, mal encadrées, pourraient s'apparenter à de la surveillance de masse.

Il sied également de relever que le Tribunal du canton de Lucerne[3] s'était prononcé sur la licéité de la prise de photographies par drones utilisées par une commune pour surveiller les constructions illicites. Le Tribunal avait retenu que la surveillance par drone - indépendamment du fait qu'elle se rapporte à des lieux publics ou privés - doit être qualifiée d'atteinte grave aux droits fondamentaux. Les juges ont qualifié les prises de vue de données personnelles sensibles, raison pour laquelle une base légale dans laquelle le but et l'étendue du traitement des données devraient être décrits dans les grandes lignes (compréhensibilité pour les personnes concernées), de même que les moyens utilisés, était nécessaire. Au regard de cet arrêt, le projet d'art. 6 n'apparaît pas de nature à respecter les exigences constitutionnelles requises en matière de base légale. Il conviendrait notamment de circonscrire les cas dans lesquels des drones pourraient être utilisés.

Quant au délai de conservation des images, il est admissible conformément à la jurisprudence en la matière. En effet, s'agissant de la question des délais de conservation des images, 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[4].

L'**art. 7** a trait à la lecture automatique de plaques d'immatriculation. Il permet à la police d'utiliser ce type de dispositif sans en préciser les finalités, ni les modalités d'utilisation. Si la durée de conservation des données est limitée et permet ainsi de réduire l'atteinte portée à la personnalité des citoyens, il conviendrait de préciser dans la loi à quelles fins les données sont collectées et dans quel cas elles seraient consultées (les explications de l'exposé des motifs ne suffisant pas à cet effet). En effet, potentiellement, il s'agit d'outils, tout comme la

[2] Le Tribunal fédéral s'est penché sur l'utilisation d'une caméra embarquée dans une voiture (privée en l'espèce) et a considéré qu'il s'agissait d'un traitement secret de données, puisque la collecte n'était pas reconnaissable (arrêt du Tribunal fédéral 6B_1188/2018, du 26 septembre 2019).
[3] Décision du Tribunal cantonal de Lucerne 7H 17 49 du 18 avril 2018, disponible sous: https://datenschutz.lu.ch/-/media/Datenschutz/Dokumente/Urteil_Kantonsgericht_Luzern_7H_17_49_18042018.pdf?la=de-CH
[4] ATF 133 I 88; voir également Cour eur. D.H., Amann, du 16 février 2000.

vidéosurveillance de lieux publics, qui peuvent s'apparenter à de la surveillance de masse, de sorte qu'ils doivent être clairement encadrés pour être compatibles avec les principes de protection des données. Telle que formulée, cette disposition donne un blanc-seing à l'utilisation de cette technologie, sans pour autant l'encadrer.

A cet égard, il convient de citer une jurisprudence du Tribunal fédéral (6B_908/2018, du 7 octobre 2019): le canton de Thurgovie avait mis en place un système de recherche automatisée de véhicules et de surveillance du trafic (RVS) qui utilise d'abord une caméra pour connaître la plaque d'immatriculation ou l'identité du détenteur; l'heure, le lieu, la direction du trajet et les occupants du véhicule sont également enregistrés. En plus de cette collecte et du stockage des informations d'identification, les données sont ensuite fusionnées avec d'autres bases de données et comparées automatiquement, ce qui permet le traitement en série et en simultané d'enregistrements de données complexes en quelques fractions de seconde. Notre Cour suprême avait relevé que les usagers de la route ne peuvent pas prévoir quelles informations seront collectées, stockées et reliées ou comparées à d'autres bases de données. En outre, le stockage et la destruction des données ne sont pas suffisamment réglementés. En particulier, la loi thurgovienne sur la police ne prévoit aucune obligation d'effacer les données immédiatement et sans laisser de traces, si aucune correspondance n'est trouvée lors de la comparaison des données. Dès lors, il avait considéré qu'en l'absence d'une base légale suffisante, les informations ainsi collectées l'ont donc été illégalement.

Selon les Préposés, cette jurisprudence permet de cerner les exigences en matière de densité normative pour l'utilisation d'un tel outil. Ils recommandent donc que la disposition soit modifiée en conséquence.

S'agissant de **l'art. 8**, les Préposés recommandent que des données anonymisées soient utilisées à des fins de formation ou de contrôle qualité et non pas les enregistrements tels quels. Ils recommandent donc de distinguer ces situations de celle de l'enregistrement intervenant à des fins de preuve. Les personnes concernées doivent être informées qu'elles sont enregistrées, ce qui est prévu, selon les explications fournies par l'exposé des motifs. L'art. 8 pourrait consister en la base légale à un enregistrement à des fins de preuve uniquement, les autres utilisations de ces enregistrements étant par ailleurs prévues par l'art. 9 du projet.

Ce qui précède s'applique également s'agissant de **l'art. 9** du projet. A l'alinéa 2, les Préposés suggèrent de supprimer les termes "si nécessaire". La personnalité des personnes concernées doit être préservée dans tous les cas.

Les **art. 12 et 13** du projet ont trait aux mesures de contrôle des accès par les membres du personnel de police. Les Préposés relèvent que la journalisation des accès répond à l'exigence de sécurité des données, puisqu'elle permet de détecter des utilisations des systèmes d'information qui ne seraient pas conformes à leur but. Toutefois, simultanément, elle implique une collecte de données des utilisateurs (agents). L'enjeu consiste à trouver un équilibre entre la surveillance intrinsèque à la journalisation et la sécurité qu'elle apporte. La durée de conservation des données de journalisation est un élément clé à cet égard qui devrait également figurer dans le projet de loi. Elle ne devrait pas excéder 6 mois, voire un an. En outre, la mise en place d'un tel système doit faire l'objet d'une information détaillée auprès des membres du personnel. Les Préposés préconisent également une consultation des associations représentatives du personnel. Des mesures de sécurité doivent en outre éviter que les informations collectées dans ce cadre puissent être utilisées à d'autres fins.

L'art. 13 du projet a trait aux contrôles préventifs nominatifs en dehors de tout soupçon d'abus. Le projet de loi instaure des cautèles pour cette pratique: un tel contrôle n'intervient que sur ordre du commandant ou de la commandante, le membre du personnel concerné en est informé, ainsi que du résultat.

L'**art. 16** concerne les droits de la personne concernée. Son alinéa 4 vise les demande d'accès portant sur le journal des évènements de la police (main-courantes). Comme l'indique l'exposé des motifs accompagnant le projet, cette disposition propose de nouvelles règles "*pour cadrer le contenu et le format des données à communiquer*". Il est précisé que le journal des évènements contient des informations à l'état brut "*correspondant aux constatations matérielles des agents et aux déclarations des parties et témoins au moment de l'événement*", ce qui implique que "*la valeur probante des informations de ce journal est toute relative*". Pour cette raison, le projet propose que l'accès soit accordé "*sous la forme d'un rapport d'information sommaire qui ne peut contenir que les informations que la police a pu vérifier ou qu'elle a constatées elle-même, à l'exclusion des simples déclarations qui lui ont été faites*". Selon l'exposé des motifs, cette solution permet de garantir l'exercice du droit d'accès à ses données personnelles tout en évitant que des informations non vérifiées ou fausses soient colportées voire utilisées à des fins ne correspondant pas aux finalités pour lesquelles elles ont été collectées.

En date du 8 janvier 2018, la Chambre administrative a rendu une décision clarifiant le statut des mains-courantes (ATA/9/2018). Cette dernière relève qu'en droit genevois, la protection des particuliers en matière de dossiers et de fichiers de police est assurée par les dispositions de la LCBVM et de la LIPAD; la question de l'accès au dossier en procédure pénale par le CPP. Au vu de ces dispositions, la Chambre administrative retient que le journal des évènements de police (main-courante) doit être considéré comme faisant partie du dossier de police. Elle conclut que par principe, s'agissant des données personnelles contenues dans les dossiers et fichiers de la police jusqu'à l'accès au dossier concédé par le CPP, l'existence d'un droit d'accès fondé sur la LIPAD entre directement en contradiction avec les restrictions prévues par le CPP, au sens de l'article 46 al. 1 litt. a LIPAD. Elle retient donc un droit d'accès différé. Dans cette affaire, aucune plainte pénale n'ayant été déposée dans le délai requis, la Chambre administrative a considéré que la police devait donner accès aux annotations faites à la main-courante concernée, dûment caviardée des données personnelles de tiers.

Les Préposés relèvent que le projet de loi restreint l'accès aux données personnelles des personnes concernées dans la mesure où, en cas de demande d'accès à une main-courante, un rapport serait établi sur la base de ladite main-courante. Un nouveau document serait ainsi créé qui contiendrait moins d'informations que le document original, soit uniquement "*les informations que la police a pu vérifier ou qu'elle a constatées elle-même, à l'exclusion des simples déclarations qui lui ont été faites*".

Bien qu'ils comprennent les raisons pratiques d'une telle modification législative, ainsi que les difficultés auxquelles la police peut être confrontée dans le caviardage des données de tiers, les Préposés ne sont pas favorables à une telle solution. En effet, elle implique intrinsèquement une limitation au droit d'accès des personnes concernées et restreint ainsi un droit qui a été confirmé par la Cour de justice. Malgré les difficultés pratiques posées par les demandes d'accès au journal des évènements de police, les Préposés sont favorables au maintien de la solution reconnue par la Cour de Justice, ce d'autant plus que la durée de conservation du journal des évènements de police est prévue pour une durée de 10 ans (art. 21 al. 4 du projet).

Le **chapitre IV** du projet de loi a trait à la communication d'informations de police à des institutions publiques. La LCBVM encadrait précisément les communications de données personnelles de police, listant les institutions destinataires ou prévoyant des conditions précises à la communication. Par ailleurs, faute de base légales spécifique, l'art. 39 LIPAD règle précisément la question de la communication de données personnelles. Cette disposition liste un certain nombre de conditions à respecter.

Le projet de loi entend faciliter cette communication, en prévoyant deux dispositions, l'une visant la communication en vertu d'une base légale et l'autre sur requête.

S'agissant de **l'art. 19** du projet, il vise la communication de données personnelles autorisée par une base légale spécifique. Dans la mesure où cette communication repose sur un autre texte légal, c'est ce dernier qui va déterminer l'ampleur de la communication et les conditions prévues. Ainsi, si la base légale sur laquelle la police entend s'appuyer pour communiquer des données ne prévoit qu'une communication sur requête, aucune communication d'office ne saurait intervenir. Les Préposés comprennent que tel est l'esprit de l'art. 19 du projet qui ne saurait aller au-delà de la base légale spécifique prévoyant la communication de données. En effet, les données de police comprenant souvent des données personnelles sensibles, une application stricte des principes de protection des données se justifie.

Concernant **l'art. 20** du projet, il a trait à la communication de données personnelles sur requête, sans qu'aucune base légale spécifique ne l'autorise. Il dispose que "*la police est autorisée à communiquer, par écrit et sur requête motivée, à d'autres autorités les données nécessaires à l'exécution des tâches qui leur sont confiées par la loi, pour autant qu'aucun intérêt privé ou public prépondérant ne s'y oppose*".

Cette disposition représente une dérogation à l'art. 11 du projet qui prévoit la confidentialité des données de police et l'interdiction de communication à des tiers non autorisés.

Les Préposés comprennent la nécessité d'une base légale spécifique dans la LIPol, la confidentialité de l'art. 11 du projet empêchant une communication de données sur la base des art. 39 et suivants LIPAD.

Il sied de souligner que les informations de police comprennent potentiellement des informations sensibles, parfois acquises dans le cadre d'enquêtes, à l'insu de la personne concernée. Les exigences en matière de densité normative sont donc particulièrement élevées quant au traitement de telles données. Pour rappel, la communication de données personnelles constitue un traitement de données personnelles. Ainsi, les principes de légalité, proportionnalité et transparence doivent être respectés.

L'exposé des motifs indique que cette disposition permettrait par exemple de communiquer des informations concernant un candidat à un poste dans l'administration cantonale, au pouvoir judiciaire ou des établissements de droit public. En d'autres termes, cette disposition permettrait ainsi une communication de toute donnée de police, y compris pour une fonction non sensible, selon la pesée des intérêts effectuée par l'institution requise. Dans l'exemple susmentionné, la communication serait contraire au principe de la proportionnalité. Un extrait de casier judiciaire pourrait simplement être requis de la part du postulant.

Ainsi, la formulation prévue par l'art. 20 du projet est trop large et ne respecte pas les exigences en matière de densité normative pour la communication de données personnelles sensibles. Elle représente un blanc-seing sur la base d'une pesée des intérêts effectuée par l'institution requise et sans aucune information à la personne concernée, alors qu'il est question de données de police, soit des données qui portent une atteinte particulière à la personnalité des personnes concernées. Les Préposés considèrent que la formulation de cette disposition doit être revue et précisée.

Les **art. 21 et 22** du projet traitent de la destruction des données personnelles. L'art. 21 du projet prévoit une destruction automatique des données après un certain laps de temps, alors que l'art. 22 permet une destruction anticipée, sur requête de la personne concernée.

Dans une affaire où un citoyen sollicitait la suppression de certaines informations de police le concernant (ATA/839/2019 du 30 avril 2019), la Cour a rappelé quelques règles en la ma-

tière: "*conformément aux exigences découlant des art. 10 al. 2 et 13 al. 2 Cst., des renseignements inexacts ne peuvent être retenus en aucun cas. En outre, dès le moment où des renseignements perdent toute utilité, leur conservation et l'atteinte que celle-ci porte à la personnalité ne se justifient plus; ils doivent être éliminés (arrêts du Tribunal fédéral 1P.713/2006 précité consid. 2; 1P.436/1989 du 12 janvier 1990 consid. 2b in SJ 1990 p. 564; ATA/636/2016 précité consid. 6c)*". Elle s'est en outre référée à la jurisprudence de la Cour européenne des droits de l'homme, selon laquelle le droit interne des États parties doit assurer que les données à caractère personnel sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire auxdites finalités (ACEDH Khelili précité, § 62; S. et Marper c. Royaume-Uni du 4 décembre 2008, req. n. 30562/04, § 103). Elle a finalement distingué entre la conservation de données d'une personne condamnée de celles relatives à une procédure pénale close par un non-lieu définitif pour des motifs de droit, un acquittement ou encore un retrait de plainte, la conservation étant conforme au principe de proportionnalité dans le premier cas (ACEDH Khelili précité, § 66; arrêt du Tribunal fédéral précité 1C_363/2014 consid. 2), mais pas dans le second (arrêt du Tribunal fédéral précité 1C_363/2014 consid. 2).

L'art. 21 du projet prévoit de manière indifférenciée la conservation des données de police, que l'infraction soit réalisée ou non. En effet, la durée de conservation est "*déterminée, pour chaque dossier par l'infraction la plus grave ou par l'infraction la plus récente, réalisée ou non*". Cette manière de calculer la durée de conservation des données n'apparaît pas compatible avec la jurisprudence susmentionnée. En effet, les données ne sauraient être conservées aussi longtemps en cas d'infraction non réalisée. L'unicité du dossier de police (art. 3 du projet) ne saurait impliquer que l'ensemble des informations concernant un individu doivent être détruites au même moment. Une telle solution serait clairement disproportionnée et pas conforme au droit supérieur.

Par ailleurs, les Préposés émettent des réserves sur la durée de conservation des informations de police, qui leur semble particulièrement longue et doutent de sa compatibilité avec la jurisprudence susmentionnée.

* * * * * *

Le projet devrait ainsi être modifié sur plusieurs points pour être pleinement compatible avec les principes de protection des données personnelles.

Les Préposés remercient la Chancellerie de les avoir consultés et se tiennent à disposition pour tout renseignement complémentaire.

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal