Requête en cessation du caractère illicite de l'atteinte

Recommandation du 14 avril 2023

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

1. Dans un courrier daté du 5 juillet 2022 adressé à la responsable LIPAD du Département de la sécurité, de la population et de la santé (DSPS), Me A. a indiqué être mandaté par B., C., D. et E., afin de défendre leurs intérêts respectifs dans le cadre de l'utilisation de *Mobile Responder* au sein de la police cantonale genevoise.

2. Il expliquait que la Direction des opérations de la police avait décidé de la mise en service de l'application *Mobile Responder* pour le 1er juillet 2022. Lui et ses mandants en avaient été informés la veille par courriel. Des contacts préalables à propos de l'application avaient eu lieu avec la Direction des opérations.

3. Selon le susnommé, *Mobile Responder* ne respecte pas les exigences en matière de protection des données personnelles prescrites par la LIPAD et son utilisation porte atteinte à la personnalité des agents qui ont l'obligation de l'utiliser. De la sorte, il conclut notamment à ce que la police: renonce à la conservation des données collectées par *Mobile Responder*, subsidiairement prenne des mesures techniques et organisationnelles pour assurer leur effacement automatique après 24h; supprime toutes les données collectées illicitement; s'abstienne de toute utilisation future de *Mobile Responder* qui ne serait pas parfaitement conforme à la directive.

4. Par pli du 4 octobre 2022 adressé à la responsable LIPAD, Me A. a requis une position du DSPS sur son précédent courrier.

5. La responsable LIPAD du Département a répondu en date du 25 octobre 2022. Selon elle, l'application respecte les principes énoncés par la LIPAD et ne porte pas atteinte à la personnalité des agents qui ont l'obligation de l'utiliser. En substance, le traitement des données de *Mobile Responder*, y compris à des fins de formation, est effectué par la police dans le cadre de l'accomplissement de ses tâches légales; la collecte (intermittente et limitée) et la conservation des données sont pertinentes et nécessaires à l'accomplissement desdites tâches; la personnalité des travailleurs est entièrement respectée.

6. Le 2 novembre 2022, Me A. s'est adressé au DSPS pour lui faire part du fait que: la proportionnalité n'est pas respectée; la conservation des données de géolocalisation n'est pas nécessaire à l'accomplissement des tâches de police; la géolocalisation n'est pas occasionnelle, mais quasi-permanente dans de nombreux cas.

7. En date du 20 février 2023, le DSPS, n'entendant pas donner suite aux prétentions des demandeurs, a fait savoir à ces derniers que la requête avait été transmise au Préposé cantonal avec ses observations, afin qu'il rende une recommandation écrite à son attention et à celle des précités.

8. Le 29 mars 2023, les Préposés ont été reçus par la Police cantonale, afin d'obtenir des explications sur l'application querellée.

9. 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* ».

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

10. Entrée en vigueur le 1er 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.

11. 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.

12. La LIPAD est applicable aux institutions publiques genevoises, en particulier aux « *établissements et corporations de droit public cantonaux et communaux, ainsi que leurs administrations et les commissions qui en dépendent* » (art. 3 al. 1 litt. c LIPAD). Le Département de la sécurité, de la population et de la santé (DSPS) 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).

13. 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.

14. 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).

15. Un profil de personnalité s'entend d'un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique (art. 4 litt. c LIPAD).

16. 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.

17. 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.

18. Selon l'art. 49 LIPAD, 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.

19. La **Directive de service DS.OSI.02.15** « *Utilisation de Mobile Responder à la Police »* a pour objectifs de formaliser les modalités d'utilisation de Mobile Responder sur smartphones et tablettes, ainsi qu'à encadrer le traitement des données des collaborateurs. Elle a la teneur suivante:

1. PRÉAMBULE

L'application informatique *Mobile Responder* est un complément du SAE utilisé par les centrales d'engagement de la police, afin d'assurer la bonne gestion du dispositif opérationnel et d'assister le personnel de police dans sa mission.

2. OBJECTIFS DE *MOBILE RESPONDER*

Les objectifs de *Mobile Responder* sont les suivants:

- Assurer la gestion opérationnelle des ressources en permettant aux centrales (CECAL, CENROUT, COPI) notamment à la CECAL de visualiser et d'optimiser le positionnement des ressources à disposition et d'améliorer la rapidité d'intervention.
- Donner aux utilisateurs une meilleure vision des réquisitions en cours.
- Transmettre des données pertinentes (textes, images, vidéos, etc.) de la CECAL vers les unités terrain ou du terrain vers la CECAL pour le traitement de réquisitions.
- Porter secours ou engager des renforts au personnel de police en danger, accidenté ou se retrouvant en difficulté lors d'une mission ou d'un engagement.
- Analyser les données rétroactives, notamment à des fins de formation et d'amélioration du dispositif opérationnel; dans ces cas de figure, les données doivent être anonymisées.
- Toute utilisation des données à des fins de surveillance est interdite.

3. DÉFINITIONS

- Unité: membre du corps de police ou véhicule.
- Utilisateur: membre du corps de police en intervention ou en opération selon la casuistique et connecté à *Mobile Responder* (cf. annexe 1).
- Données de géolocalisation: coordonnées géographiques de la position (latitude et longitude en degrés) d'un terminal (tablettes ou téléphone mobile) laquelle est actualisée à intervalles réguliers. Ces données sont enregistrées dans une base de données de manière séquentielle.
- Statut opérationnel: code qui indique la disponibilité et l'activité en cours.
- Logs techniques: désignent l'enregistrement chronologique des évènements survenant au niveau des composants informatiques de *Mobile Responder*. Ces logs servent au bon fonctionnement de l'application en permettant de corriger les éventuels dysfonctionnements techniques. Ils ne peuvent être analysés que par l'OCSIN ou HEXAGON et à des fins ne se rapportant pas à des personnes.
- Logs métier: désignent le relevé chronologique des opérations informatiques effectuées par les utilisateurs de *Mobile Responder* pendant le fonctionnement de l'application (exemples: statut opérationnel, disponibilité, création et suivi d'évènements, appel de détresse, etc.). Ces logs permettent d'assurer la traçabilité, l'imputabilité et la non-répudiation des actions effectuées par les

utilisateurs. Les durées de conservation des différents logs sont traitées au point 6.5.

- Se connecter / déconnecter (log-in / log-out): démarrer *Mobile Responder* en cliquant sur l'icône et en introduisant son identifiant personnel ou du véhicule (en s'assurant que la géolocalisation est activée dans les paramètres du terminal). La déconnexion se fait par le menu de *Mobile Responder*.

4. DÉPLOIEMENT

Mobile Responder est installé sur toutes les tablettes véhicules et sur les smartphones de dotation des membres du corps de police équipés.

5. RÈGLES D'ENGAGEMENT

5.1. Véhicules police

Mobile Responder doit être activé sur les tablettes de tous les véhicules en service, équipés, en introduisant l'identifiant et le mot de passe définis dans l'application, selon les directives et la doctrine d'utilisation de l'application (se référer à l'annexe 1).

5.2. Personnel de la Police

Tous les membres du corps de police habilités, assurant des missions explicitées dans la doctrine d'utilisation de *Mobile Responder* (se référer à l'annexe 1) ont l'obligation de se connecter à *Mobile Responder* en introduisant l'identifiant et le mot de passe définis dans l'application dès qu'ils quittent les bureaux.

Les exceptions et dérogations peuvent être octroyées par le Chef de service.

Par exemple:

- Policiers en patrouille (véhicule, pédestre, équestre, navigation, motards, …).
- Policiers en mission administrative mais pouvant être engagés en cas d'urgence.
- ASP effectuant des missions opérationnelles.
- Policiers effectuant des enquêtes sur le terrain.
- Personnel administratif engagé dans une mission (par exemple BPTS).

La doctrine d'utilisation de l'application détaillée dans la casuistique est annexée à cette directive (se référer à l'annexe 1).

Le personnel n'entrant pas dans la doctrine d'utilisation, ne doit pas se connecter à dans *Mobile Responder*.

Au terme de la mission, le personnel doit se déconnecter de *Mobile Responder*.

Les actions de connexion/déconnexion ne sont pas automatiques. Une action manuelle de la part de l'utilisateur est requise.

En cas d'oubli de déconnexion, une demande d'effacement des logs portant sur la période hors doctrine d'utilisation peut être formulée au chef de service.

Fonctionnalités principales:

- Création d'un événement terrain: la création d'un événement est faite directement depuis l'application (statut opérationnel "sur place" automatique).
- Suivi de l'événement: permet de suivre en temps réel le déroulement d'une opération.
- Gestion des statuts opérationnels: les utilisateurs renseignent leur statut ("en route", "sur place", etc.) afin que les centrales d'engagement de la police connaissent l'état des ressources à disposition.

- Réalisation d'appels de "détresse": en appuyant sur un bouton pendant 3 secondes, un appel est relayé automatiquement auprès des centrales d'engagement.
- Activation et désactivation de *Mobile Responder* selon la doctrine d'utilisation de l'application annexée à cette directive.

Pour davantage d'informations, se référer au manuel d'utilisation de *Mobile Responder*.

6. PROTECTION DES DONNÉES

L'utilisation de *Mobile Responder* s'effectue conformément aux dispositions de la LIPAD et aux principes décrits ci-dessous. Pour rappel, les données personnelles collectées dans les logs sont, au sens de la LIPAD, le nom d'utilisateur et l'identifiant de l'appareil.

6.1. Collecte des données

La collecte des données par *Mobile Responder* commence dès la connexion à l'application et se termine à la déconnexion (actions manuelles déclenchées uniquement par l'utilisateur). Aucune donnée n'est collectée lorsque l'application est déconnectée. La connexion ou la déconnexion à *Mobile Responder* ne peut être effectuée que par le membre du corps de police concerné, conformément à la doctrine d'utilisation de l'application.

L'état de l'application (activé ou non) est clairement visible sur l'application (trois carrés verts si activé).

Les données enregistrées sont les suivantes:

- Les identifiants de connexion: nom d'utilisateur / numéro du véhicule.
- Les dates et heures (activation / désactivation).
- Le terminal sur lequel *Mobile Responder* est activé.
- Les coordonnées de géolocalisation relevées.
- Le statut opérationnel.

Le tableau de la fréquence d'enregistrement de la position dans les logs se trouve sous l'annexe 2.

6.2. Finalité du traitement des données

Les données, en particulier celles indiquant la géolocalisation, ne sont analysées que dans la mesure où leur traitement permet d'atteindre les buts définis au chapitre 2.

Les données peuvent être utilisées anonymisées, sur autorisation du Chef OP, à des fins de formation ou pour améliorer le dispositif.

6.3. Proportionnalité de la collecte

Seules peuvent être collectées les données personnelles nécessaires à atteindre les buts prédéfinis au chapitre 2 et rappelés au point 6.1 ci-dessus.

Ces données peuvent uniquement être collectées durant les réquisitions et les missions opérationnelles, selon les règles d'engagement.

6.4. Sécurité des données

L'OCSIN, le SSI et le CCSIP s'assurent que des mesures techniques et organisationnelles adéquates sont mises en place pour garantir que le traitement des données de *Mobile Responder* soit effectué de manière à assurer le respect de cette directive et la sécurité des données.

6.5. Durées de conservation

- Les logs métiers, y compris les données de géolocalisation (voir chapitre 3 Définitions) sont conservées durant une période de 100 jours pour les tablettes dans les véhicules et 30 jours pour les smartphones.
- Les logs techniques (voir chapitre 3 Définitions) sont conservés pendant le temps nécessaire défini par la politique de backup de l'OCSIN.

6.6. Confidentialité des données

Les données collectées sont traitées de manière confidentielle. Toute utilisation contraire aux buts définis au chapitre 2 ci-dessus est interdite.

Seul le CDT ou un membre de l'état-major désigné en son absence peut consulter les données.

6.7. Droit de consultation des données personnelles

Les utilisateurs disposent du droit de consulter toutes les données personnelles collectées par *Mobile Responder* qui les concernent.

Les demandes d'accès sont adressées par écrit au CDT. A réception d'une demande, le CDT rend sans délai un ordre de préservation pour s'assurer que la demande puisse être traitée conformément à la LIPAD.

7. RÔLES ET RESPONSABILITÉS

Le Chef OP met en œuvre les règles et la doctrine d'utilisation de l'application dans la casuistique et les ordres d'engagement.

8. GESTION DES RISQUES ET CONTRÔLE QUALITÉ

Le SRQI procède, une fois par année à des revues pour s'assurer notamment que:

- Le traitement des données est effectué conformément aux principes de protection des données personnelles indiqués au point 6 ci-dessus.
- Les données sont systématiquement et effectivement supprimées à l'expiration de leur durée maximale de conservation.
- Les ordres de préservation et les accès aux données étaient justifiés.
- La doctrine d'utilisation (annexe 1) est scrupuleusement respectée.
- Les éventuels risques liés à la sécurité de l'application sont identifiés et traités, si nécessaire. Le SRQI procède ou fait procéder à une nouvelle analyse des risques pour vérifier que l'application satisfait aux conditions de sécurité requises.

Les résultats des revues et contrôles font l'objet d'un rapport détaillé qui est transmis au CDT par le chef du SRQI.

Annexe 1 à la directive sur Mobile Responder

DOCTRINE D'UTILISATION DE MOBILE RESPONDER		
MISSIONS	Enrôlement	COMMENTAIRES
Déplacement hors canton	**Non**	cours, visites, …
FOI - FOCO	**Non**	cours de formation
Enquêtes sur le terrain	**Oui**	pénales, de proximité, par délégation d'un service officiel (SMC, OCIRT, …), …
Missions de circulation	**Oui**	flux, positionnement, …
Missions diplomatiques	**Oui**	positionnement des entités
Missions administratives	**Oui**	type de missions qui permettent d'être engagé en cas d'urgence

Patrouilles	**Oui**	pour disposer du maillage terrain
Zone aéroportuaire	**Oui**	positionnement des entités
Manifestations	**Sur ordre**	positionnement des chefs de section et entités (MO, TP, Eagle, circulation, planton, …)
Opération diverses	**Sur ordre**	filature, observation, surveillance, interpellation, DéFI, …
Ordre public	**Sur ordre**	positionnement des entités

Annexe 2 à la directive sur Mobile Responder

Tableau des fréquences d'envoi des positions GPS par statut (si Mobile Responder est activé)

Statut	Code statut	actualisation (secondes)
Disponible	DI (08)	10
Régulé	RE	10
En Route	DP (01)	10
Arrivé	SP (02)	10
Hors Service	HS	30
Indisponible	AD	300

Précision de la géolocalisation:

La précision a été évaluée sur le terrain à environ 20 mètres.

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

20. En préambule, les Préposés observent que, dès 2006, une grande majorité des véhicules de police était équipée d'un système de géolocalisation dénommée Carloc, qui transmettait ses données au travers du réseau mobile 2G de Swisscom, abandonné le 15 février 2021. C'est précisément pour pallier cette obsolescence que l'application *Mobile Responder* a été choisie.

21. Cette dernière a été déployée le 1er juillet 2022 sur les smatphones (iphones de dotation) et les tablettes police (ipad dans les voitures de patrouille). Elle constitue un module du SAE (Système d'aide à l'engagement) utilisé par les centrales pour gérer l'opérationnel du terrain, soit notamment créer des réquisitions, attribuer des patrouilles, transmettre des informations, positionner les forces pour assurer des barrages et des bouclages.

22. S’agissant des règles d’engagement (art. 5.1 et 5.2 de la Directive), l’application est installée sur toutes les tablettes véhicules et sur les smartphones de dotation des membres du corps de police équipés. Elle doit être activée sur les tablettes de tous les véhicules en service équipés, en introduisant l'identifiant et le mot de passe définis dans l'application. Tous les membres du corps de police habilités, assurant des missions explicitées dans la doctrine d'utilisation de *Mobile Responder* (selon l'annexe 1) ont l'obligation de se connecter à *Mobile Responder* en introduisant l'identifiant et le mot de passe définis dans l'application dès qu'ils quittent les bureaux. En d’autres termes, concrètement, les policiers en patrouille doivent loguer leur véhicule et leur équipage dans le système, renseigner leur statut (libre, en route, mission administrative, etc.) et se géolocaliser. Au terme de la mission, le personnel doit se déconnecter de *Mobile Responder.*

23. L’application a pour objectifs, selon le ch. 2 de la Directive: d’assurer la gestion opérationnelle des ressources en permettant aux centrales (CECAL, CENROUT, COPI), notamment à la CECAL, de visualiser et d'optimiser le positionnement des ressources à disposition et d'améliorer la rapidité d'intervention; de donner aux utilisateurs une meilleure vision des réquisitions en cours; de transmettre des données pertinentes (textes, images, vidéos, etc.) de la CECAL vers les unités terrain ou du terrain vers la CECAL pour le traitement de réquisitions; de porter secours ou engager des renforts au personnel de police en danger, accidenté ou se retrouvant en difficulté lors d’une mission ou d'un engagement; d’analyser les données rétroactives, notamment à des fins de formation et d’amélioration du dispositif opérationnel; dans ces derniers cas de figure, les données doivent être anonymisées. Il est précisé que *« Toute utilisation des données à des fins de surveillance est interdite* ».

24. Les requérants ne remettent pas en cause ces objectifs. En revanche, selon eux, l'application ne serait pas conforme aux principes de protection des données consacrés par les art. 35 ss LIPAD, et ce sur différents aspects qui seront repris dans l'analyse ci-dessous.

25. La Directive contient un chapitre 6 dédié la protection des données. Il est précisé que l'utilisation de *Mobile Responder* s'effectue conformément aux dispositions de la LIPAD.

26. En premier lieu, les Préposés relèvent que les données collectées par l’application sont les suivantes: identifiants de connexion: nom d'utilisateur/numéro du véhicule; dates et heures (activation/désactivation); terminal sur lequel *Mobile Responder* est activée; coordonnées de géolocalisation relevées; statut opérationnel (art. 6.1 de la Directive). Les données de localisation des véhicules constituent des données personnelles, car elles se rapportent à des personnes physiques (les policiers) identifiables ou identifiées.

27. Conformément à l’art. 6.1 de la Directive, la collecte des données par l’application commence dès la connexion et se termine à la déconnexion (actions manuelles déclenchées uniquement par l'utilisateur). Aucune donnée n’est collectée lorsque l’application est déconnectée. La connexion ou la déconnexion ne peut être effectuée que par le membre du corps de police concerné, conformément à la doctrine d’utilisation de l’application. L’état de l’application (activé ou non) est clairement visible sur l'application (trois carrés verts si activé).

28. Selon l’art. 6.5 de la Directive, les logs métiers, y compris les données de géolocalisation sont conservées durant une période de 100 jours pour les tablettes dans les véhicules et 30 jours pour les smartphones. Les logs techniques sont conservés pendant le temps nécessaire défini par la politique de backup de l'OCSIN.

29. S'agissant de **la base légale**, les requérants estiment que « *La collecte (chaque 10 secondes) et la conservation (pendant des semaines voire des mois) des données de déplacement des policiers sont des traitements de données de déplacement des policiers et peuvent constituer des profils de personnalité. La directive n'est pas une loi formelle ni une loi matérielle bénéficiant d'une délégation de compétence. Elle fait référence à de nombreux textes légaux, sans qu'il soit clairement possible d'identifier la base légale utilisée. De plus, aucune ne semble permettre un traitement à des fins de formation* ». Le DSPS considère au contraire que la collecte et la conservation des données sont conformes à la mission de la police.

30. Les missions de la police sont énumérées à l'art. 1 LPol (notamment assurer l'ordre, la sécurité et la tranquillité publics ou encore prévenir la commission d'infractions et veiller au respect des lois). Pour les Préposés, les données collectées, afférentes aux déplacements des policiers et à leur localisation lorsqu'ils sont en service, le sont conformément à celles-ci. Il s'agit de données de géolocalisation collectées de manière intermittente lorsque les policiers sont sur le terrain, soit seulement pendant une partie de leur journée de travail. Ces données ne sont pas de nature à permettre d'apprécier les caractéristiques essentielles de la personnalité des agents; elles ne constituent donc pas des profils de personnalité. Il n'est ainsi pas indispensable d'élaborer une base légale pour l'application querellée. Il suffit, conformément à l'art. 36 LIPAD, que les données soient pertinentes et nécessaires à l'accomplissement des tâches légales de la police, ce qui est le cas au vu de l'art. 1 LPol.

31. L'art. 31 LPol traite de la formation et du développement personnel. La police a, de la sorte, également comme tâche légale de former les candidats aux fonctions de policier et d'assistant de sécurité publique. La Directive (art. 2) prévoit certes la possibilité d'analyser les données rétroactives à des fins de formation et d'amélioration du dispositif opérationnel. Cela étant, les Préposés sont d'avis que, pour un tel objectif, seules des données anonymisées peuvent entrer en ligne de compte. L'on ne voit pas en quoi des données non anonymisées seraient pertinentes pour une telle finalité. D'ailleurs, l'art. 6.2 de la Directive prévoit que les données peuvent être utilisées anonymisées à des fins de formation ou pour améliorer le dispositif. Il convient ainsi de remplacer le terme « *peuvent* » par celui de « *doivent* ».

32. S'agissant du **principe de finalité**, les Préposés notent que l'adverbe notamment, qui figurait à l'art. 2, laissant penser que d'autres buts, non indiqués, auraient pu être envisagés, en contradiction avec l'exigence de prévisibilité et de transparence, a été supprimé.

33. Selon l'art. 6.3 de la Directive, relatif au **principe de proportionnalité**, seules peuvent être collectées les données personnelles nécessaires à atteindre les buts prédéfinis au chapitre 2 et rappelés au point 6.1. Ces données peuvent uniquement être collectées durant les réquisitions et les missions opérationnelles, selon les règles d'engagement. Pour les requérants, ce principe ne serait pas respecté: « *La possibilité d'utilisation rétroactive des données de l'application à des fins de formation et d'amélioration du dispositif apparaît beaucoup plus problématique, puisqu'il implique la conservation jusqu'à 100 jours de données personnelles, y compris de géolocalisation. (30 jours pour smartphones, 100 jours pour tablettes). Ces durées sont clairement excessives. Elles ne sont ni nécessaires ni utiles à atteindre les buts visés; ceux-ci exigent en effet des données en temps réel* ». Au contraire, selon le DSPS, « *… les policiers ne sont tenus d'activer l'application que lorsque, dans le cadre de l'accomplissement de leurs activités contractuelles, ils se trouvent dans les situations prévues par l'annexe 2 de la directive ad hoc. D'ailleurs le nombre total de licences d'utilisation ne dépasse pas 250, y compris les licences utilisées dans les véhicules. Cela signifie qu'il ne peut pas y avoir plus de 250 personnes et véhicules connectées en même temps. D'ailleurs, d'après les tests*

effectués, il y a une moyenne de 300 sessions (une connexion suivie d'une déconnexion) par journée (24 heures). Sachant qu'une même personne se connecte et se déconnecte plusieurs fois dans la journée, en fonction de ses activités, il apparaît clairement que l'utilisation de l'application n'est ni massive ni générale ni permanente, mais partielle et intermittente ».

34. Il convient d'apprécier concrètement la proportionnalité des durées de conservation des données au regard de la finalité pour laquelle l'application *Mobile Responder* est utilisée, en mettant en balance, d'une part, l'intérêt public de la police à conserver pendant une durée limitée (30-100 jours) des données personnelles collectées dans le but de satisfaire à des obligations légales et, d'autre part, l'intérêt des collaborateurs à ne pas voir leurs données de géolocalisation traitées en dehors du temps réel. Les Préposés notent à cet égard que l'application est installée sur les téléphones de dotation fournis par la police cantonale et sur des tablettes installées dans des véhicules de police dont l'usage est strictement professionnel; il ne s'agit donc pas d'instruments privés. *Mobile Responder* sert l'intérêt public à disposer de véhicules et de personnel policier pour protéger et servir la population, en cas de besoin, mais pourrait également servir à localiser une patrouille en difficulté. Cela étant, pour les Préposés, la durée de conservation prévue est excessive et non justifiée, puisque les circonstances particulières (à savoir la finalité pour laquelle *Mobile Responder* est utilisée) nécessitent de connaître la position et la disponibilité des policiers en temps réel, non plusieurs jours après. Un traitement en temps réel des données apparaît suffisant pour atteindre les buts précités. Pour des raisons opérationnelles, un effacement des données après 24h peut être considéré comme adéquat. Un traitement plus long des données personnelles doit être considéré comme disproportionné. Seules des données anonymisées pourraient être conservées plus longtemps à des fins de formation, comme susmentionné.

35. S'agissant du principe de **sécurité des données**, l'art. 6.4 de la Directive énonce que « *L'OCSIN, le SSI et le CCSIP s'assurent que des mesures techniques et organisationnelles adéquates sont mises en place pour garantir que le traitement des données de Mobile Responder soit effectué de manière à assurer le respect de cette directive et la sécurité des données* ». Les Préposés n'ont pas eu accès aux mesures techniques et organisationnelles mentionnées, ni aux contrats signés par le DSPS. Ils ne sont donc pas en mesure de se prononcer sur le respect de ce principe. Ils encouragent toutefois le DSPS à s'assurer que ce principe est respecté.

36. Enfin, les Préposés observent que le grief relatif au **respect de la personnalité des travailleurs** sort du cadre de la mission qui leur échoit. Cela étant, ils remarquent que, selon le Tribunal fédéral, « *Un système de surveillance est interdit par l'art. 26 OLT 3 s'il vise uniquement ou essentiellement à surveiller le comportement comme tel des travailleurs. En revanche, son utilisation n'est pas prohibée si, bien qu'emportant objectivement un tel effet de surveillance, il est justifié par des raisons légitimes, tels des impératifs de sécurité ou des motifs tenant à l'organisation ou à la planification du travail ou encore à la nature même des relations de travail. Encore faut-il, cependant, que le système de surveillance choisi apparaisse, au vu de l'ensemble des circonstances, comme un moyen proportionné au but poursuivi, et que les travailleurs concernés aient préalablement été informés de son utilisation* » (ATF 130 II 425, cons. 4.4).

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande au Département de la sécurité, de la population et de la santé, concernant l'application *Mobile Responder*:

- De modifier la **Directive de service DS.OSI.02.15** « *Utilisation de Mobile Responder à la Police* » de sorte qu'elle prévoie que « *sont prises des mesures techniques et organisationnelles pour assurer l'effacement automatique des données collectées après 24h* ».
- De modifier la **Directive de service DS.OSI.02.15** « *Utilisation de Mobile Responder à la Police* » de sorte qu'elle prévoie que seules des données anonymisées peuvent être analysées rétroactivement à des fins de formation et d'amélioration du dispositif opérationnel.
- De prendre toutes les mesures pour s'assurer que le principe de sécurité des données personnelles est respecté.

Dans les 10 jours à compter de la réception de la présente recommandation, le Département de la sécurité, de la population et de la santé doit rendre une décision sur les prétentions des requérants (art. 49 al. 6 LIPAD).

La présente recommandation est notifiée par pli recommandé à:

- Me A. ….
- 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

Stéphane Werly
Préposé cantonal

Joséphine Boillat
Préposée adjointe

Pour rappel, conformément à l'art. 49 al. 6 LIPAD, l'institution publique notifie une copie de sa décision au Préposé cantonal à la protection des données et à la transparence.