RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

POUVOIR JUDICIAIRE

A/2271/2023-DIV **ATA/422/2024**

COUR DE JUSTICE

Chambre administrative

Arrêt du 26 mars 2024

dans la cause

A_____
B_____
C_____
D_____ **recourants**
représentés par Mes Sylvain MÉTILLE et Marie-Laure PERCASSI, avocats

contre

DÉPARTEMENT DES INSTITUTIONS ET DU NUMÉRIQUE

et

PRÉPOSÉ CANTONAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE **intimés**

EN FAIT

A. **a.** L'D_____ (ci-après : D_____) est une association, ayant son siège à Genève, représentant les membres issus des services de gendarmerie (police-secours, police de proximité, police routière et divers services de la police cantonale), ainsi que les agents de détention et les inspecteurs de l'office cantonal des véhicules (ci-après : OCV).

À teneur des statuts, dans leur teneur entrée en vigueur le 1er janvier 2023 (ci-après : les statuts), elle a pour but de veiller au respect des droits syndicaux des membres par une couverture en assurance juridique et la défense de leurs conditions de travail et salariales. Elle cultive la solidarité et favorise l'entraide et la camaraderie (art. 3 statuts). Les membres sont : a) les fonctionnaires du corps de police ; b) l'inspectorat de l'OCV ; c) les agents de détention, rattaché à un statut de fonctionnaire normal ou particulier ainsi que tout membre du personnel pénitentiaire ; d) ainsi que leurs retraités, à certaines conditions.

b. Le C_____ (ci-après : C_____) est une association, ayant également son siège à Genève, regroupant les policiers de la police judiciaire de Genève et visant à la culture de l'esprit de camaraderie et de solidarité, ainsi qu'à la défense professionnelle de ses membres.

Peuvent être admis comme membres actifs, les inspecteurs et gradés de la police judiciaire, de l'état-major de police et du commissariat de police, s'ils en remplissent les conditions. D'autres membres peuvent être admis si leur admission représente un intérêt pour le C_____.

c. A_____, policier, et B_____, officier de police judiciaire, sont tous deux membres de respectivement l' D_____ et du C_____ en tant que présidents.

d. Dès 2006, la majorité des véhicules de police était équipée d'un système de géolocalisation nommé CARLOC, lequel avait pour but de les localiser et d'engager de manière efficace les patrouilles de police sur le terrain. Les données issues de CARLOC étaient conservées pendant 122 jours.

Le 1er juillet 2022, ce système devenu obsolète a été remplacé par l'application MOBILE RESPONDER (ci-après : l'application), laquelle est installée sur toutes les tablettes des véhicules de police et sur les téléphones portables de dotation des policiers afin de les géolocaliser.

B. **a.** À partir du printemps 2021, des discussions et échanges de courriels ont eu lieu au sujet de la prochaine utilisation de l'application entre l'D_____, le C_____ et la direction des opérations de la police (ci-après : DIROP).

b. Le 1er juillet 2022, l'application a été mise en œuvre et la directive DS OSI.02.15 sur l'utilisation de l'application à la police (ci-après : la directive) est entrée en vigueur.

Selon celle-ci, l'application était utilisée « 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 » (art. 1). Les objectifs de l'application étaient précisés, dont celui d'« analyser les données rétroactives, notamment à des fins de formation et d'amélioration du dispositif opérationnel ; dans ce cas de figure, les données [devaient], dans la mesure du possible, être anonymisées », étant précisé que « toute utilisation des données à des fins de surveillance [était] interdite » (art. 2). Elle était installée « sur toutes les tablettes véhicules et sur les smartphones de dotation des membres du corps de police » (art. 4). Les données enregistrées par l'application étaient les suivantes : « les identifiants de connexion (nom d'utilisateur/numéro de véhicule), les dates et heures (activation/désactivation), le terminal sur lequel l'application était activée, les coordonnées de géolocalisation relevées et le statut opérationnel » (art. 6.1). « La durée de conservation des données de connexion [était] de 30 jours pour les téléphones portables et 100 jours pour les tablettes se trouvant dans les véhicules de service » (art. 6.5). « Les données collectées étaient traitées de manière confidentielle. Seul le commandant ou un membre de l'état-major désigné en son absence [pouvait] consulter les données » (art. 6.6).

c. Par courrier du 5 juillet 2022, l'D_____, le C_____, A_____ et B_____ ont demandé à la responsable selon la loi sur l'information du public et l'accès aux documents du 5 octobre 2001 (LIPAD - A 2 08 ; ci-après : responsable LIPAD) du département de la sécurité, de la population et de la santé, devenu depuis lors le département des institutions et du numérique (ci-après : le département), à titre provisionnel et sans délai :

- de suspendre le déploiement de l'application jusqu'à l'entrée en force de la décision de la police et de renoncer à exploiter les données déjà collectées ;

- de renoncer à la conservation de données collectées par l'application, subsidiairement de prendre des mesures techniques et organisationnelles pour assurer leur effacement automatique après 24 heures, de supprimer toutes les données collectées illicitement et de s'abstenir de toute utilisation future de l'application qui ne serait pas parfaitement conforme à la directive.

L'application ne respectait pas les exigences en matière de protection des données prescrites par la LIPAD et son utilisation portait atteinte à la personnalité des policiers devant l'utiliser. La directive ne reposait sur aucune base légale claire le permettant. Les durées de conservation prévues étaient excessives. Les art. 2, 6.2 et 6.6 de la directive n'étaient pas formulés de manière conforme. L'application constituait un moyen de surveillance constante qui ne protégeait pas suffisamment la personnalité des policiers concernés.

d. S'en sont suivis divers échanges de correspondance entre la D_____, le C_____, A_____ et B_____, d'une part, et le département, d'autre part.

Ce dernier a notamment accepté de changer certains termes figurant aux art. 2 et 6 de la directive.

Ces modifications demeurant insuffisantes pour l'D_____, le C_____, A_____ et B_____, ceux-ci ont demandé au département la transmission de leur requête au préposé cantonal à la protection des données et à la transparence (ci-après : PPDT).

e. Le 14 avril 2023, le PPDT a recommandé au département de :

- modifier la directive, de sorte que celle-ci prévoie que « soient prises les mesures techniques et organisationnelles pour assurer l'effacement automatique des données collectées après 24 heures+ » et 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 était respecté.

Les données de localisation des véhicules constituaient des données personnelles, car elles se rapportaient à des personnes physiques (les policiers) identifiables ou identifiées. Les données collectées, afférentes aux déplacements des policiers et à leur localisation lorsqu'ils étaient en service, l'étaient conformément aux missions de la police énumérées à l'art. 1 de la loi sur la police du 9 septembre 2014 (LPol - F 1 05). Ces données n'étant pas de nature à permettre d'apprécier les caractéristiques essentielles de la personnalité des policiers, elles ne constituaient pas des profils de personnalité. Conformément à l'art. 36 LIPAD, il suffisait qu'elles fussent pertinentes et nécessaires à l'accomplissement des tâches légales de la police. Vu l'art. 31 LPol, seules des données anonymisées pouvaient être utilisées à des fins de formation. L'adverbe « notamment » figurant à l'art. 2 de la directive pouvait laisser penser que d'autres buts, non indiqués, auraient pu être envisagés, en contradiction avec l'exigence de prévisibilité et de transparence. L'application servait 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, la durée de conservation prévue était excessive et non justifiée, puisque les circonstances particulières nécessitaient de connaître la position et la disponibilité des policiers en temps réel, non plusieurs jours après. Pour des raisons opérationnelles, un effacement des données au-delà de 24 heures pouvait être considéré comme disproportionné. Seules des données anonymisées pourraient être conservées plus longtemps à des fins de formation. Le PPDT n'avait pas eu accès aux mesures techniques et organisationnelles, ni aux contrats signés par le département, de sorte qu'il n'était pas en mesure de se prononcer sur le respect du principe de sécurité. Le grief relatif au respect de la personnalité des travailleurs sortait du cadre de sa mission.

f. Par décision du 8 juin 2023, le département a :

- refusé de modifier la directive dans le sens d'assurer un effacement automatique des données collectées après 24 heures ;

- accepté la recommandation prévoyant que seules les données anonymisées pouvaient être analysées rétroactivement à des fins de formation et d'amélioration du dispositif technique, avec réserve car les données collectées ne seraient anonymisées que pour autant qu'elles doivent servir à des fins de formation et d'amélioration du dispositif technique. Les données enregistrées devant être extraites à des fins pénales ne seraient pas anonymisées ;

- considéré que la recommandation visant à prendre toutes les mesures pour s'assurer du respect du principe de sécurité était sans objet, les standards de sécurité étant garantis et vérifiés régulièrement au travers d'audits de sécurité ;

- refusé de suspendre le déploiement de l'application jusqu'à l'entrée en force de la décision de police au sens de l'art. 49 al. 6 LIPAD ;

- refusé de renoncer à exploiter les données déjà collectées, celles-ci étant détruites à l'expiration du délai de conservation applicable au moment de la collecte ;

- refusé la suppression des données collectées, au motif qu'elles auraient été collectées illicitement ;

- rejeté l'abstention de toute utilisation future de l'application qui serait conforme à la directive, dans la mesure où elle était sans objet.

g. Le 14 juin 2023, la directive a été mise à jour et communiquée aux membres du personnel de police.

Les modifications apportées étaient les suivantes :

- art. 2 de la directive : dans les objectifs de l'application, avec l'ajout comme objectif de « fournir les moyens de preuve utiles dans le cadre d'une procédure pénale » et la suppression des termes « notamment » et « dans la mesure du possible » dans la finalité « analyser les données rétroactives, notamment à des fins de formation et d'amélioration du dispositif opérationnel ; dans ce cas de figure, les données doivent être anonymisées » ;

- art. 6.2 de la directive : les données de géolocalisation étaient transmises exclusivement à l'autorité de poursuite pénale, respectivement au service de police en charge de l'enquête. Seules des données anonymisées pouvaient être utilisées à des fins de formation ou pour améliorer le dispositif ;

- art. 6.5 de la directive : la durée de la conservation des « logs » (données de géolocalisation enregistrées) de l'application sur les téléphones de dotation du personnel de la police était portée de 30 à 100 jours, comme pour les tablettes des véhicules de police.

C. **a.** Par acte du 6 juillet 2023, l'D_____, le C_____, A_____ et B_____ ont recouru auprès de la chambre administrative de la Cour de justice (ci-après : la chambre administrative) contre la décision du 8 juin 2023, en concluant

principalement, à son annulation, à ce qu'il soit ordonné au département de prendre les mesures techniques et organisationnelles afin que les données collectées par l'application soient effacées automatiquement après 24 heures, de supprimer les données déjà collectées dont la durée de conservation avait déjà dépassé 24 heures et de modifier la directive afin que celle-ci respectât les précédentes conclusions. Subsidiairement, ils sollicitaient le renvoi de la cause au département pour nouvelle décision. À titre provisionnel, ils demandaient qu'il soit ordonné au département de suspendre la sauvegarde des données collectées par l'application au-delà d'une durée de 24 heures et de supprimer les données déjà collectées et conservées depuis plus de 24 heures jusqu'à droit connu sur le fond.

La qualité pour recourir, notamment celle de l'D_____ et du C_____, devait être admise.

La restriction du droit à la sphère privée entraînée par la collecte et la conservation de données personnelles via l'application était grave. Une base légale cantonale formelle faisait défaut, dès lors que la LPol ne contenait aucune disposition relative au traitement des données personnelles des agents de police. Une directive était insuffisante. L'art. 1 LPol ne pouvait pas être considéré comme une base légale suffisante au regard de l'art. 35 LIPAD quant à l'objectif de « fournir des moyens de preuve utiles dans le cadre d'une procédure pénale ». La conservation pendant 100 jours des données de géolocalisation n'était ni apte ni nécessaire pour atteindre les finalités visées par la directive. Le but de formation pouvait être atteint avec des données anonymisées. Les données de géolocalisation n'étaient généralement pas pertinentes pour déterminer si un policier avait commis une infraction. À l'inverse, le risque pour les policiers que la hiérarchie utilise les données collectées en violation de la directive qui interdisait la surveillance, pour les sanctionner, était important. Des moyens permettant de disculper les policiers visés par des plaintes existaient déjà et étaient suffisants pour prouver leur innocence. L'application était avant tout utilisée en temps réel pour connaître la position des patrouilles et améliorer les interventions de la police.

La nouvelle finalité ajoutée par le département à la directive et l'augmentation de la durée de conservation des données collectées par l'application, ne leur avaient pas été communiquées avant le prononcé de la décision contestée, de sorte qu'ils n'avaient pas eu l'occasion de faire valoir leur point de vue à ce sujet. Cette manière d'agir permettait au département de contourner la procédure prévue par la LIPAD et de soustraire ces ajouts au contrôle du PPDT.

Était notamment joint un article de presse du 6 mai 2023, relatant les propos de la commandante de la police, mentionnant notamment que, entre 2014 et 2022, 249 plaintes à l'encontre de policiers avaient été enregistrées et seules sept d'entre elles avaient abouti à la condamnation du policier après enquête.

b. Le département a conclu au rejet de la demande de mesures provisionnelles.

La qualité pour recourir de l'D_____ était discutable dans la mesure où il ne semblait pas qu'il puisse être considéré que la majorité du syndicat fût constituée de policiers actifs.

La mise en œuvre de l'application permettait de diminuer le délai de conservation des données à 100 jours. Les données de géolocalisation issues de l'application pourraient servir tant en faveur qu'en défaveur des policiers, injustement accusés. La hiérarchie policière n'utilisait pas les données tirées de l'application pour exercer une surveillance. C'était seulement lorsque l'Inspection générale des services (ci-après : IGS) ou le procureur général découvraient, dans le cadre de leurs investigations liées à une procédure pénale, des manquements aux devoirs de service qu'ils les communiquaient à la commandante de la police, laquelle y donnait la suite qu'ils comportaient en termes disciplinaires.

Les recourants ne démontraient pas en quoi leur intérêt à ce que les données enregistrées par l'application fussent effacées après 24 heures serait prépondérant par rapport à celui de l'État à la manifestation de la vérité et à réaliser une instruction efficace des procédures pénales, ainsi qu'à l'intérêt privé prépondérant des recourants à ce qu'ils puissent être disculpés en cas de procédure pénale. Les données récoltées par l'intermédiaire de l'application étaient des données issues de GPS, soit des données satellitaires. Elles étaient bien plus précises que des données GSM, générées par les tablettes et téléphones portables qui étaient fonction de la présence d'antennes à proximité et la triangulation pour l'établissement d'une géolocalisation. Les données issues de l'application n'étaient utilisées que dans un nombre restreint de situations.

c. Les recourants ont répliqué sur mesures provisionnelles.

L'application concernait les policiers en fonction qui constituaient la majorité des membres de l'D_____.

Il ne pouvait être déduit de la durée de conservation des données issues de CARLOC une quelconque légalité à la conservation des données de l'application pendant 100 jours. La finalité ajoutée ne pouvait pas servir à justifier la durée de conservation de données personnelles : en cas contraire, toutes les données personnelles devraient être conservées pendant la durée nécessaire au dépôt d'une plainte pénale.

d. Par décision présidentielle du 25 août 2023 (ATA/905/2023), la chambre administrative a rejeté la requête de mesures provisionnelles.

La qualité pour recourir des recourants s'analyserait avec l'arrêt au fond.

e. Le département a conclu au rejet du recours. Il s'en rapportait à l'appréciation de la chambre administrative quant à la recevabilité de celui-ci pour ce qui concernait l'D_____.

L'application était utilisée uniquement dans le cadre professionnel et de manière intermittente. L'enclenchement de l'application au départ d'une mission et la

déconnexion à son terme étaient effectués par les collaborateurs de la police eux-mêmes. Les statistiques d'utilisation révélaient que le nombre de collaborateurs connectés était très faible. Les 250 licences acquises par la police pour l'utilisation de l'application, tablettes de véhicules comprises, ne permettaient pas de connexions au-delà de ce nombre. Ce dernier était inférieur au nombre de collaborateurs de la police dotés de téléphones portables sur lesquels l'application était installée. L'enregistrement et la conservation des données de géolocalisation avaient lieu uniquement pendant le temps d'exécution de certaines missions spécifiques énumérées dans la directive.

Dans la mesure où les données collectées n'étaient pas des données personnelles sensibles ni des profils de personnalité, l'art. 35 LIPAD constituait une base légale suffisante pour les traiter aussi longtemps qu'elles se révèleraient pertinentes et nécessaires à l'accomplissement des tâches légales ayant nécessité leur collecte, soit le délai de plainte de trois mois.

L'ajout d'une finalité supplémentaire et du rallongement de la durée de conservation des données collectées lorsque l'application était installée sur le téléphone professionnel avait été effectué le 14 juin 2023, soit après la prise de la décision du 8 juin 2023, et avait pour but d'apporter une clarification supplémentaire. La recommandation du PPDT ne limitait pas le pouvoir du département lequel n'avait fait que rendre une décision conformément à l'art. 49 al. 6 LIPAD. La directive n'était pas une décision mais représentait des instructions de la direction de la police à ses collaborateurs. Elle n'avait ainsi pas à être soumise préalablement aux collaborateurs mais l'était parfois à bien plaire. Une éventuelle violation du droit d'être entendu pouvait être réparée par-devant la chambre administrative.

Au surplus, il se référait à ses précédentes écritures.

f. Dans leur réplique, les recourants ont persisté dans leurs conclusions et précédents développements. Ils sollicitaient la consultation du PPDT.

La protection de la vie privée et des données personnelles s'appliquait également aux activités professionnelles. Le département n'avait fourni aucun document permettant de constater que la police n'avait que 250 licences et n'avait pas produit de statistiques d'utilisation. Il n'était donc pas possible de savoir combien de personnes étaient régulièrement connectées à l'application. Certains grands événements pouvaient mobiliser plus de 200 policiers, de sorte qu'il y aurait plus de 250 utilisations simultanées. Le besoin de géolocaliser les policiers, notamment pour leur sécurité et la bonne marche de la police, ne serait alors pas rempli, ce qui signifiait que ce déploiement n'était pas nécessaire, à tout le moins pas de manière aussi systématique que l'exigeait la doctrine d'engagement.

De nombreuses infractions étaient poursuivies d'office, de sorte que le délai de conservation de 100 jours n'était pas apte à atteindre le but visé, à savoir fournir des preuves dans une procédure pénale. L'éventuel but dissuasif de l'application

était limité, vu qu'il n'existait pas de risque significatif que des agents de police commettent des infractions pénales graves.

g. Le PPDT a maintenu sa position telle qu'exprimée dans sa recommandation précitée.

En outre, il renvoyait à sa position initiale, à savoir que la directive soit modifiée afin de prévoir que « sont prises des mesures techniques et organisationnelles pour assurer l'effacement automatique des données collectées après 24h ».

L'application était utilisée pour assurer la bonne gestion du dispositif opérationnel de la police lors de missions. Les données de géolocalisation étaient collectées dans ce but. L'ajout d'une finalité relative à la conservation de moyens de preuve potentiels en cas de dépôt de plainte pénale pourrait être invoquée dans n'importe quel contexte et pour toutes les données traitées par les institutions publiques. Or, cela serait contraire au principe de la proportionnalité, selon lequel la nécessité d'un traitement de données devait répondre à un besoin effectif.

h. Les recourants ont encore ajouté que, comme la présente procédure concernait également la protection de la personnalité des travailleurs, notamment celle des policiers, et que l'D_____ et le C_____ défendaient les intérêts de ces professionnels, leur qualité pour recourir devait leur être reconnue sur la base de l'art. 58 de la loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce du 13 mars 1964 (LTr - RS 822.11).

i. Sur quoi, les parties ont été informées que la cause était gardée à juger.

EN DROIT

1. Le recours a été interjeté en temps utile devant la juridiction compétente (art. 132 de la loi sur l'organisation judiciaire du 26 septembre 2010 - LOJ - E 2 05 ; art. 62 al. 1 let. a de la loi sur la procédure administrative du 12 septembre 1985 - LPA - E 5 10).

2. À titre liminaire, il convient d'examiner la qualité pour recourir de l'D_____, celle-ci étant remise en cause par l'autorité intimée.

2.1 À teneur de l'art. 60 al. 1 let. a et b LPA, les parties à la procédure qui a abouti à la décision attaquée et toute personne qui est touchée directement par une décision et a un intérêt personnel digne de protection à ce qu'elle soit annulée ou modifiée, sont titulaires de la qualité pour recourir (ATA/1254/2022 du 13 décembre 2022 consid. 3a et les arrêts cités). La chambre administrative a déjà jugé que les let. a et b de la disposition précitée doivent se lire en parallèle : ainsi, le particulier qui ne peut faire valoir un intérêt digne de protection ne saurait être admis comme partie recourante, même s'il était partie à la procédure de première instance (ATA/905/2022 du 6 septembre 2022 consid. 3b et l'arrêt cité).

2.2 Selon la jurisprudence, le recourant doit être touché de manière directe, concrète et dans une mesure et avec une intensité plus grandes que la généralité des administrés, et l'intérêt invoqué, qui n'est pas nécessairement un intérêt juridiquement protégé, mais qui peut être un intérêt de fait, doit se trouver, avec l'objet de la contestation, dans un rapport étroit, spécial et digne d'être pris en considération (ATF 143 II 506 consid. 5.1 ; arrêt du Tribunal fédéral 1C_593/2019 du 19 août 2020 consid. 1.2). En application de ces principes, le recours d'un particulier ou d'une association, formé dans l'intérêt général ou d'un tiers, est irrecevable (ATF 138 II 162 consid. 2.1.1 ; arrêt du Tribunal fédéral 1C_61/2019 du 12 juillet 2019 consid. 1.2 ; ATA/23/2021 du 12 janvier 2021 consid. 4). Ces exigences ont été posées de manière à empêcher l'action populaire proscrite en droit suisse (arrêt du Tribunal fédéral 2C_61/2019 du 21 janvier 2019 consid. 3.1). Il faut donc que le recourant ait un intérêt pratique à l'admission du recours, soit que cette admission soit propre à lui procurer un avantage de nature économique, matérielle ou idéale (ATF 143 II 578 consid. 3.2.2.2 ; arrêt du Tribunal fédéral 1C_536/2021 consid. 1 ; ATA/303/2023 du 23 mars 2023 consid. 2a). Un intérêt purement théorique à la solution d'un problème est de même insuffisant (ATF 144 I 43 consid. 2.1).

Une association jouissant de la personnalité juridique est autorisée à former un recours en son nom propre lorsqu'elle est touchée dans ses intérêts dignes de protection (art. 60 al. 1 let. a et b LPA et 89 al. 1 let. c de la loi fédérale sur le Tribunal fédéral du 17 juin 2005 - LTF - RS 173.110).

Une association peut faire valoir les intérêts de ses membres lorsqu'il s'agit d'intérêts qu'elle doit statutairement protéger, qui sont communs à la majorité ou à un grand nombre de ses membres et que chacun a qualité pour s'en prévaloir à titre individuel, aussi nommé « recours corporatif égoïste » (ATF 145 V 128 consid. 2.2 ; 137 II 40 consid. 2.6.4 ; 131 I 198 consid. 2.1 ; arrêt du Tribunal fédéral 2C_52/2009 du 13 janvier 2010 consid 1.2.2, non publié in ATF 136 I 1). Ces conditions doivent être remplies cumulativement ; elles doivent exclure tout recours populaire. Celui qui ne fait pas valoir ses intérêts propres, mais uniquement l'intérêt général ou l'intérêt public, n'est pas autorisé à recourir. Le droit de recours n'appartient par conséquent pas à toute association qui s'occupe, d'une manière générale, du domaine considéré. Il doit au contraire exister un lien étroit et direct entre le but statutaire de l'association et le domaine dans lequel la décision litigieuse a été prise (JdT 2011 p. 286 consid. 1.1.1 et les références citées). En revanche, elle ne peut prendre fait et cause pour l'un de ses membres ou pour une minorité d'entre eux (ATF 145 V 128 consid. 2.2 ; 142 II 80 consid. 1.4.2 ; arrêt du Tribunal fédéral 2C_749/2021 du 16 mars 2022 consid. 1.2.1 ; ATA/1064/2022 du 18 octobre 2022 consid. 5b).

Ont aussi qualité pour recourir les organisations auxquelles la loi reconnaît le droit de recourir (art. 60 al. 1 let. e LPA et 89 al. 2 let. d LTF).

En matière de protection de la santé des travailleurs, l'employeur est tenu de prendre toutes les mesures nécessaires pour protéger la santé et l'intégrité personnelle des travailleurs (art. 6 al. 1 LTr, disposition applicable aux administrations cantonales en vertu de l'art. 3a let. a LTr). La protection de l'intégrité personnelle des travailleurs correspond à la protection de la personnalité prévue à l'art. 328 de la loi fédérale du 30 mars 1911, complétant le Code civil suisse (CO, Code des obligations - RS 220 ; secrétariat d'État à l'économie [ci-après : SECO], Commentaire article par article de la LTr et ses ordonnances, novembre 2006, p. 2 ad art. 6, disponible sur https://www.seco.admin.ch/seco/fr/home/Arbeit/Arbeitsbedingungen/Arbeitsgesetz-und-Verordnungen/Wegleitungen/wegleitung-zum-arg.html#-151879252, consulté le 14 mars 2024). Dans ce cadre, l'art. 58 LTr donne également la qualité pour recourir contre les décisions des autorités cantonales et fédérales prises en exécution de la LTr aux associations des employeurs et des travailleurs intéressés.

2.3 La chambre de céans a déjà jugé que la qualité pour agir d'une association ne saurait être appréciée une fois pour toutes. Il convient notamment de vérifier, périodiquement au moins, si les conditions d'existence des associations sont réalisées, si les buts statutaires sont en rapport avec la cause litigieuse et si la décision d'ester en justice a bien été prise par l'organe compétent (ATA/1064/2022 précité consid. 5d et les arrêts cités).

Dans ses arrêts ATA/1017/2023 du 19 septembre 2023 (consid. 1.3.3) et ATA/1077/2023 du 3 octobre 2023 (consid. 3.5), la chambre de céans a admis la qualité pour recourir de l'D_____ en application de l'art. 58 LTr en tant qu'association veillant à la défense des conditions de travail de ses membres dont faisait partie, *in casu*, le personnel pénitentiaire, s'agissant de procédure visant, selon l'autorité intimée, à protéger l'intégrité des agents.

2.4 En l'occurrence, il n'est pas contesté que l'D_____, au même titre que les autres recourants, est destinataire de la décision querellée.

Conformément à ses statuts, l'D_____ représente et défend les intérêts de ses membres, lesquels sont principalement constitués par les différents corps de police, soit des policiers. Ces derniers sont directement concernés par l'installation de l'application sur leur téléphone de dotation et les tablettes des véhicules de police, celle-ci visant à les géolocaliser personnellement en temps réel.

Dès lors que la majorité des membres de l'D_____ sont des policiers appelés à utiliser l'application dans le cadre de leurs fonctions, il y a lieu de retenir que cette association dispose de la qualité pour recourir.

En outre, si, contrairement à ce qui a été indiqué dans l'ATA/1017/2023 précité, il ne s'agit pas ici de protéger la santé des policiers *stricto sensu* par l'utilisation de *bodycams*, mais principalement de géolocaliser les patrouilles de police afin d'assurer l'efficacité de leurs interventions, il n'en demeure pas moins que celle-ci vise leurs conditions de travail, en particulier sous l'angle de la protection de la

personnalité et de l'intégrité personnelle au sens de l'art. 6 LTr. Par conséquent, la qualité pour recourir doit également être reconnue à l'D_____ sous l'angle de l'art. 58 LTr.

Au surplus, la qualité pour recourir des autres recourants n'est, à juste titre, pas contestée.

Par conséquent, le recours est également recevable de ce point de vue.

3. Le recours porte sur la conformité au droit de la décision de l'autorité refusant : a) de réduire la durée de conservation des données collectées à 24 heures et d'ordonner leur effacement automatique après cette durée ; b) de renoncer à la conservation des données non anonymisées à des fins pénales et à exploiter les données déjà collectées avant l'expiration du délai de conservation alors applicable ; et c) de supprimer les données collectées au motif qu'elles l'auraient été illicitement.

Postérieurement à la notification de ladite décision, l'autorité intimée a encore modifié la directive en question en ajoutant un but à son art. 2 et en modifiant la durée de conservation des données collectées à son art. 6.5, de 30 à 100 jours pour les téléphones portables, la durée de 100 jours étant inchangée pour les tablettes se trouvant dans les véhicules de police.

4. En premier lieu, les recourants font valoir une violation de leur droit d'être entendus au motif que l'autorité intimée a modifié la directive après la notification de la décision querellée, de sorte qu'eux-mêmes et le PPDT n'ont pu se prononcer sur les modifications apportées.

4.1 Tel qu'il est garanti par l'art. 29 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst. - RS 101), le droit d'être entendu comprend notamment le droit pour l'intéressé d'offrir des preuves pertinentes et d'obtenir qu'il y soit donné suite (ATF 132 II 485 consid. 3.2 ; 127 I 54 consid. 2b). Ce droit ne s'étend qu'aux éléments pertinents pour l'issue du litige et n'empêche pas le juge de renoncer à l'administration de certaines preuves et de procéder à une appréciation anticipée de ces dernières, s'il acquiert la certitude que celles-ci ne l'amèneront pas à modifier son opinion ou si le fait à établir résulte déjà des constatations ressortant du dossier (ATF 138 III 374 consid. 4.3.2 ; 131 I 153 consid. 3).

4.2 En vertu de l'art. 47 al. 1 LIPAD, toute personne physique ou morale de droit privé peut, à propos des données la concernant, exiger des institutions publiques qu'elles s'abstiennent de procéder à un traitement illicite (let. a) ; mettent fin à un traitement illicite et en suppriment les effets (let. b) ; constatent le caractère illicite du traitement (let. c). Toute requête fondée sur les art. 44, 47 ou 48 LIPAD doit être adressée par écrit au responsable chargé de la surveillance de l'organe dont relève le traitement considéré (art. 49 al. 1 LIPAD).

Le responsable saisi traite la requête avec célérité (art. 49 al. 2 phr. 1 LIPAD). S'il n'entend pas faire droit intégralement aux prétentions du requérant ou en cas de

doute sur le bien-fondé de celles-ci, il transmet la requête au préposé cantonal avec ses observations et les pièces utiles (art. 49 al. 4 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 (art. 49 al. 5 LIPAD). L'institution concernée statue alors par voie de décision dans les dix jours sur les prétentions du requérant. Elle notifie aussi sa décision au préposé cantonal (art. 49 al. 6 LIPAD).

Bien qu'elle ne soit pas contraignante ni pour le destinataire ni pour les responsables du traitement qui se livrent à des traitements semblables ou même identiques, la recommandation est dotée d'une force morale importante, car elle émane d'une autorité publique spécialisée (Atenas ANDERSON/Benedetta S. GALETTI, La conservation des données personnelles : comment déterminer sa durée ?, in Sic! 2021, p. 117).

4.3 Par ailleurs, il convient de rappeler le droit d'information et de consultation des travailleurs et de leurs représentants sur les affaires concernant les questions relatives à la protection de la santé (art. 48 al. 1 let. a LTr), le droit d'être consulté comprenant le droit d'être entendu sur ces affaires et d'en débattre avant que l'employeur ne prenne une décision, ainsi que le droit d'obtenir communication des motifs de la décision prise lorsque les objections soulevées par les travailleurs ou leurs représentants dans l'entreprise n'ont pas été prises en considération, ou qu'elles ne l'ont été que partiellement (art. 48 al. 2 LTr).

4.4 En l'espèce, dès le printemps 2021, des discussions et des échanges de courriels ont eu lieu entre la DIROP et les recourants au sujet de l'installation de l'application. Après que celle-là a fait part aux recourants des modifications apportées au projet de directive et leur en a transmis une copie, les intéressés ont manifesté auprès du responsable LIPAD leur désaccord sur certains points de la directive, en particulier la durée de conservation de données collectées. Nonobstant ces circonstances, ce n'est que face à l'insistance des recourants que l'autorité intimée a finalement fait appel au PPDT.

Cependant, le département n'a pas suivi la recommandation du PPDT sur les points contestés les plus problématiques. Il ne lui a pas non plus permis, ainsi qu'aux recourants, de se prononcer sur les modifications apportées à la directive subséquemment à la notification de la décision querellée, alors que celles-ci portaient sur des points contestés, notamment l'ajout d'une finalité, la durée de la conservation des données de géolocalisation collectées et leur anonymisation.

Il ressort du déroulement de ces faits que, non seulement, l'autorité intimée a tardé à faire appel au PPDT et n'y a procédé que sur relance de la part des recourants, mais également qu'elle ne leur a pas permis de se prononcer sur les nouvelles modifications de la directive, adoptées postérieurement à la notification de la décision litigieuse.

Force est de constater qu'en procédant de la sorte, le département n'a pas respecté le droit d'être entendu des recourants. D'une part, il n'a pas satisfait au déroulement de la procédure prévue par la LIPAD. D'autre part, il n'a pas permis la mise en œuvre du droit d'information et de consultation des recourants, tel que prévu par l'art. 48 LTr.

Il s'ensuit que l'autorité intimée a violé leur droit d'être entendus.

Cela étant, compte tenu du pouvoir d'examen de la chambre de céans, du fait que tant le PPDT que les recourants ont pu respectivement se déterminer et faire valoir leurs arguments dans le cadre de la présente procédure, y compris sur les modifications de la directive, il y a lieu de considérer que dite violation a été réparée.

Par conséquent, ce grief sera écarté.

5. En second lieu, les recourants invoquent une violation de leur droit à la sphère privée, ainsi qu'une violation de la procédure relative à la LIPAD en matière de protection des données personnelles.

Ces deux perspectives impliquent, qu'il s'agisse d'une éventuelle atteinte à la sphère privée ou d'un manquement en matière de protection de données personnelles, qu'une définition de ces notions doit être apportée, afin d'examiner si les points contestés de la directive reposent sur une base légale, sont justifiés par un intérêt public prépondérant et sont proportionnés par rapport aux finalités visées.

Dès lors, afin d'éviter la répétition d'un raisonnement susceptible d'être applicable pour ces deux approches, les griefs des recourants seront traités cumulativement (arrêt du Tribunal fédéral 2C_230/2010 du 12 avril 2010 consid. 3.2 et 3.7).

5.1.1 Tout être humain a droit à la liberté personnelle, notamment à l'intégrité physique et psychique et à la liberté de mouvement (art. 10 al. 2 Cst.). Toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications (art. 13 al. 1 Cst.). Le droit au respect de la vie privée et familiale est également garantie par l'art. 8 § 1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 (CEDH - RS 0.101).

La protection de l'intégrité personnelle des travailleurs prévue à l'art. 6 al. 1 LTr correspond à la protection de la personnalité à l'art. 328 CO, qui protège notamment la santé des travailleurs et leur intégrité physique et psychique, ainsi que leur sphère privée, leur image, leur dignité, ou encore certaines libertés personnelles (ATF 130 II 425 consid. 3.2 et 3.3 ; SECO, op. cit., p. 2 ad art. 6). Il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail (art. 26 al. 1 de l'ordonnance 3 relative à la LTr (protection de la santé) du 18 août 1993 - OLT 3 - RS 822 113). Lorsque des systèmes de surveillance ou de contrôle sont nécessaires pour d'autres raisons, ils

doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs (art. 26 al. 2 OLT 3).

Il est veillé à la protection de la personnalité des membres du personnel (art. 2B al. 1 *ab initio* de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux du 4 décembre 1997 - LPAC - B 5 05 ; art. 1 al. 1 du règlement relatif à la protection de la personnalité à l'État de Genève du 12 décembre 2012 - RPPers - B 5 05.10). Des mesures sont prises pour prévenir, constater et faire cesser toute atteinte à la personnalité (art. 2B al. 2 LPAC ; art. 1 al. 2 RPPers). Est constitutive d'une atteinte à la personnalité toute violation illicite d'un droit de la personnalité, telles notamment la santé physique et psychique, l'intégrité morale, la considération sociale, la jouissance des libertés individuelles ou de la sphère privée (art. 3 al. 1 RPPers).

5.1.2 La notion de « vie privée » au sens de l'art. 8 CEDH est une notion large, qui ne se prête pas à une définition exhaustive. Elle recouvre l'intégrité physique et morale d'une personne ainsi que de multiples aspects de son identité physique et sociale (ACEDH López Ribalda et autres c. Espagne du 17 octobre 2019, req. n^{os} 1874/13 et 8567/13, § 87 ; Denisov c. Ukraine du 25 septembre 2018, req. n^{o} 76639/11, § 95, 25 septembre 2018). Elle englobe notamment des éléments d'identification d'un individu tels que son nom ou sa photographie (ACEDH López Ribalda et autres c. Espagne du 17 octobre 2019, req. n^{os} 1874/13 et 8567/13, § 87 ; Schüssel c. Autriche du 21 février 2002, req. n^{o} 42409/98, 21 février 2002).

La notion de vie privée ne se limite pas à un « cercle intime », où chacun peut mener sa vie personnelle sans intervention extérieure, mais englobe également le droit de mener une « vie privée sociale », à savoir la possibilité pour l'individu de nouer et de développer des relations avec ses semblables et le monde extérieur (ACEDH Bărbulescu c. Roumanie du 5 septembre 2017, req. n^{o} 61496/08, § 70). À ce titre, elle n'exclut pas les activités professionnelles (ACEDH Antović et Mirković c. Monténégro du 28 novembre 2017, req. n^{o} 70838/13, § 42) ni les activités qui ont lieu dans un contexte public. Il existe en effet une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée (ACEDH López Ribalda et autres c. Espagne du 17 octobre 2019, req. n^{os} 1874/13 et 8567/13, § 88 et les arrêts cités).

Un certain nombre d'éléments entrent en ligne de compte lorsqu'il s'agit de déterminer si la vie privée d'une personne est touchée par des mesures prises en dehors de son domicile ou de ses locaux privés. Puisqu'à certaines occasions les gens se livrent sciemment ou intentionnellement à des activités qui sont ou peuvent être enregistrées ou rapportées publiquement, ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur significatif, quoique pas nécessairement décisif. S'agissant de la surveillance des actions d'un individu au moyen de matériel photo ou vidéo, les organes de la CEDH ont ainsi estimé que la surveillance des faits et gestes d'une

personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constituait pas en elle-même une forme d'ingérence dans la vie privée. En revanche, des considérations tenant à la vie privée peuvent surgir dès lors que des données à caractère personnel, notamment les images d'une personne identifiée, sont recueillies et enregistrées de manière systématique ou permanente. Comme la Cour l'a souligné à cet égard, l'image d'un individu est l'un des attributs principaux de sa personnalité, parce qu'elle exprime son originalité et lui permet de se différencier de ses pairs. Le droit de chaque personne à la protection de son image constitue ainsi l'une des conditions essentielles de son épanouissement personnel et présuppose principalement la maîtrise par l'individu de son image. Si pareille maîtrise implique dans la plupart des cas la possibilité pour l'individu de refuser la diffusion de son image, elle comprend en même temps le droit pour lui de s'opposer à la captation, la conservation et la reproduction de celle-ci par autrui (ACEDH López Ribalda et autres c. Espagne du 17 octobre 2019, req. n^{os} 1874/13 et 8567/13, § 89 ; Reklos et Davourlis c. Grèce du 15 janvier 2009, req. n^{o} 1234/05, § 40).

Pour déterminer si l'art. 8 CEDH trouve à s'appliquer, la question de savoir si l'individu en cause a été ciblé par la mesure de surveillance ou si des informations à caractère personnel ont été traitées, utilisées ou rendues publiques d'une manière ou dans une mesure excédant ce à quoi les intéressés pouvaient raisonnablement s'attendre est pertinente (ACEDH López Ribalda et autres c. Espagne du 17 octobre 2019, req. n^{os} 1874/13 et 8567/13 § 90 et les arrêts cités).

5.1.3 En parallèle, la LIPAD régit l'information relative aux activités des institutions et la protection des données personnelles (art. 1 al. 1 LIPAD). Elle poursuit deux objectifs, à savoir, d'une part, favoriser la libre formation de l'opinion et la participation à la vie publique ainsi que, d'autre part, protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant (art. 1 al. 2 let. a et b LIPAD).

La LIPAD comporte deux volets. Le premier concerne l'information du public et l'accès aux documents ; il est réglé dans le titre II (art. 5 ss LIPAD). Le second porte sur la protection des données personnelles, dont la réglementation est prévue au titre III (art. 35 ss LIPAD). À l'origine, elle se limitait au seul aspect de l'information du public et de l'accès aux documents (MGC 2000 45/VIII 7641 ss et MGC 2001 49/X 9678 ss relatifs au projet de loi 8'356 sur l'information du public et l'accès aux documents ; ATA/1404/2017 du 17 octobre 2017 consid. 2 et les arrêts cités). Le volet portant sur la protection des données personnelles résulte d'un deuxième processus législatif initié, le 7 juin 2006, par le dépôt d'un projet de loi 9'870 sur la protection des données personnelles (MGC 2005-2006 X A 8448 ss), qui est devenu, au cours des travaux législatifs, un projet visant à modifier la LIPAD en y intégrant le volet relatif à la protection des données personnelles (MGC 2007-2008 XII A 14079 ss, en particulier 14137 ss).

La LIPAD s'applique notamment aux pouvoirs exécutif, législatif et judiciaire cantonaux, ainsi qu'à leurs administrations et aux commissions qui en dépendent (art. 3 al. 1 let. a LIPAD).

5.2.1 Comme tout droit fondamental, les droits à la liberté personnelle et à la protection de la sphère privée peuvent être restreints à certaines conditions. Selon l'art. 36 Cst., toute restriction d'un droit fondamental doit être fondée sur une base légale. Les restrictions graves doivent être prévues par une loi. Les cas de danger sérieux, direct et imminent sont réservés (al. 1). Toute restriction d'un droit fondamental doit être justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui (al. 2) et être proportionnée au but visé (al. 3). L'essence des droits fondamentaux est inviolable (al. 4).

En vertu de l'art. 8 § 2 CEDH, il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit à la protection de la vie privée et familiale que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

5.2.2 Selon le Tribunal fédéral, les restrictions graves d'un droit fondamental supposent une base claire et explicite dans une loi au sens formel (art. 36 al. 1 2e phr. Cst.). Pour les restrictions légères, une loi au sens matériel suffit. Les dispositions doivent être formulées d'une manière suffisamment précise pour permettre aux individus d'adapter leur comportement et de prévoir les conséquences d'un comportement déterminé avec un degré de certitude approprié aux circonstances. Le degré de précision exigible ne peut pas être défini abstraitement. Il dépend notamment de la diversité des états de faits à régler, de la complexité et de la prévisibilité de la décision à prendre dans le cas d'espèce, des destinataires de la règle, de l'intensité de l'atteinte portée aux droits fondamentaux, et finalement de l'appréciation de la situation qui n'est possible que lors de l'examen du cas individuel et concret (ATF 139 I 280 = JdT 2014 I 118 consid. 5.1 et les arrêts cités).

Les mots « prévue par la loi » au sens de l'art. 8 § 2 CEDH veulent d'abord dire que la mesure incriminée doit avoir une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle et sa compatibilité avec la prééminence du droit. Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention (ACEDH Fernández Martínez c. Espagne du 12 juin 2014, req. no 56030/07, § 117).

5.2.3 Dans la même perspective, l'art. 35 LIPAD prévoit que les institutions publiques ne peuvent traiter des données personnelles que si, et dans la mesure où, l'accomplissement de leurs tâches légales le rend nécessaire (al. 1). Des données personnelles sensibles ne peuvent être traitées que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée (al. 2).

Par données personnelles ou données, la LIPAD vise toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable (art. 4 let. a LIPAD). Par ailleurs, constitue un traitement de ces données toute opération relative à celles-ci – quels que soient les moyens et procédés utilisés – notamment leur collecte, conservation, exploitation, modification, communication, archivage ou destruction (art. 4 let. e LIPAD). La communication est définie comme le fait de rendre accessibles des données personnelles ou un document, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant (art. 4 let. f LIPAD).

5.3.1 La notion d'intérêt public, au sens de l'art. 36 al. 2 Cst., varie dans le temps et selon le lieu et comprend non seulement les biens de police (tels que l'ordre, la sécurité, la santé et la tranquillité publics, etc.), mais aussi les valeurs culturelles, écologiques et sociales dont les tâches de l'État sont l'expression. Ces intérêts publics se concrétisent généralement dans le cadre d'un processus politique de l'adoption démocratique des lois, laquelle ne s'opère pas de manière arbitraire mais à la lumière du système de valeur de l'ordre juridique global. Ils doivent en outre constituer un critère de restriction pertinent pour la limitation du droit fondamental en cause. Si ce droit ne peut pas être restreint pour les motifs invoqués par la collectivité publique, ces motifs n'entrent pas en considération à titre d'intérêt public pertinent (ATF 142 I 49 = JdT 2016 I 67 consid. 8.1 et les arrêts cités).

5.3.2 L'art. 8 § 2 CEDH mentionne la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, et la protection des droits et libertés d'autrui.

5.4 Le principe de la proportionnalité ancré à l'art. 36 al. 3 Cst. exige que la mesure envisagée soit apte à produire les résultats d'intérêt public escomptés (règle de l'aptitude) et que ceux-ci ne puissent être atteints par une mesure moins incisive (règle de la nécessité). En outre, elle interdit toute limitation allant au-delà du but visé et postule un rapport raisonnable entre celui-ci et les intérêts publics ou privés compromis (principe de la proportionnalité au sens étroit, impliquant une pesée des intérêts ; ATF 148 I 160 consid. 7.10 ; 140 I 218 consid. 6.7.1). La restriction ne doit pas être plus grave que nécessaire d'un point de vue objectif, spatial, temporel et personnel. Les intérêts antagonistes privés et publics doivent être évalués et pondérés en considération des circonstances de l'espèce et du contexte social actuel (ATF 142 I 49 = JdT 2016 I 67 consid. 9.1 et les arrêts cités).

Selon l'art. 8 § 2 CEDH, toute ingérence dans l'exercice du droit à vie privée et familiale doit être nécessaire dans une société démocratique. Une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants » (ACEDH Fernández Martínez c. Espagne du 12 juin 2014, req. nº 56030/07, § 124).

5.4.1 Concernant la qualité des données personnelles, l'art. 36 LIPAD précise que les institutions publiques veillent, lors de tout traitement de données personnelles, à ce que ces dernières soient : pertinentes et nécessaires à l'accomplissement de leurs tâches légales (let. a) ; exactes et si nécessaire mises à jour et complétées, autant que les circonstances permettent de l'exiger (let. b ; al. 1). Lorsqu'une institution publique constate que des données personnelles qu'une autre institution lui a communiquées en vertu de l'art. 39 al. 1 LIPAD, sont inexactes, incomplètes ou obsolètes, elle en informe cette dernière, à moins que cette information ne soit contraire à une loi ou à un règlement (al. 2).

5.4.2 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 (art. 40 al. 1 LIPAD). Sur décision de l'instance dirigeante de l'institution publique concernée, la destruction de données personnelles peut être différée durant deux ans au maximum à des fins d'évaluation de politiques publiques. Ces données sont dès lors soustraites à communication, sauf si elles sont accessibles au regard de la loi sur les archives publiques, du 1er décembre 2000, ou du titre II de la LIPAD (art. 40 al. 2 LIPAD).

5.4.3 Aux termes de l'art. 41 LIPAD, dans le cadre de l'accomplissement de leurs tâches légales, les institutions publiques sont en droit de traiter des données personnelles à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques, pour leur propre compte ou celui d'une autre institution publique en ayant la mission légale, aux conditions cumulatives que : le traitement de données personnelles soit nécessaire à ces fins (let. a) ; ces données soient détruites ou rendues anonymes dès que le but du traitement spécifique visé le permet (let. b) ; les données collectées à ces seules fins ne soient communiquées à aucune autre institution, entité ou personne (let. c) ; les résultats de ce traitement ne soient le cas échéant publiés que sous une forme excluant la possibilité d'identifier les personnes concernées (let. d) ; le préposé cantonal en soit préalablement informé avec les précisions utiles sur le traitement qu'il est prévu de faire des données personnelles et sa nécessité (let. e) ; le traitement portant sur des données personnelles sensibles ou impliquant l'établissement de profils de la personnalité fasse préalablement l'objet d'une autorisation du Conseil d'État, qui doit requérir le préavis du préposé cantonal et assortir au besoin sa décision de charges ou conditions (let. f ; al. 1). Les compétences et les règles de

fonctionnement de la Cour des comptes sont réservées, de même que celles de l'office cantonal de la statistique (al. 2).

5.4.4 En matière de protection des données, l'exploitant ne peut collecter et traiter que les données qui sont aptes, mais surtout objectivement nécessaires pour atteindre le but poursuivi, pour autant que le traitement demeure dans un rapport raisonnable entre le résultat (légitime) recherché et le moyen utilisé, tout en préservant le plus possible les droits des personnes concernées. Il faut ainsi à chaque fois procéder à une pondération des intérêts entre le but du traitement et l'atteinte nécessaire à la personnalité, ce qui oblige à prendre en compte également les intérêts de l'auteur du traitement (Philippe MEIER, Protection des données, fondements, principes généraux et droit privé, Berne, 2011, n° 666 ; Atenas ANDERSON/Benedetta S. GALETTI, *op. cit.*, p. 105).

La nécessité d'un traitement ne peut être instituée en règle. Celui-ci doit répondre à un besoin effectif, et non pas simplement théorique ou relativement éloigné. C'est là ce qu'impose la proportionnalité de principe. La collecte ou la conservation de données « pour le cas où… » n'est pas admissible, sauf disposition légale spéciale (Philippe MEIER, *op. cit.*, n° 671).

La durée de la conservation peut elle aussi violer le principe de la proportionnalité dans sa portée temporelle, lorsqu'elle va au-delà de ce que nécessite le traitement, sans qu'il existe un motif justificatif (comme la nécessité de documenter à des fins de preuve). Le maître du fichier a l'obligation de détruire les données ou de les anonymiser dès qu'elles ne sont plus nécessaires à la réalisation de la tâche pour laquelle elles ont été collectées (Philippe MEIER, *op. cit.*, n° 679).

À cet égard, la chambre de céans a d'ores et déjà considéré dans son arrêt ATA/190/2012 du 3 avril 2012 en matière de radiation de données personnelles dans les dossiers de police, que le droit interne devait assurer que celles-ci soient pertinentes et non excessives par rapport aux finalités pour lesquelles elles étaient enregistrées, et qu'elles étaient conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire auxdites finalités (consid. 6 et les références citées).

Par ailleurs, la personne au sujet de laquelle des informations ont été recueillies a en principe le droit de consulter les pièces consignant ces renseignements afin de pouvoir réclamer leur suppression ou leur modification s'il y a lieu ; ce droit découle de l'art. 10 al. 2 Cst., qui garantit la liberté personnelle, et plus spécifiquement de l'art. 13 al. 2 Cst. qui protège le citoyen contre l'emploi abusif de données personnelles. La conservation de renseignements dans les dossiers de police porte en effet une atteinte au moins virtuelle à la personnalité de l'intéressé car ces renseignements peuvent être utilisés ou consultés par les agents de la police, être pris en considération lors de demandes d'informations présentées par certaines autorités, voire être transmis à ces dernières (ATF 137 I 167 consid. 3.2 ; 126 I 7 consid. 2a ; arrêt du Tribunal fédéral 1C_580/2019 du 12 juin 2020 consid. 2).

5.5 Au titre de ses missions, la police est au service de la population, dont elle reflète la diversité. Sa devise est : protéger et servir (art. 1 al. 1 LPol). En tout temps, le personnel de la police donne l'exemple de l'honneur, de l'impartialité, de la dignité et du respect des personnes et des biens. Il manifeste envers ses interlocuteurs le respect et l'écoute qu'il est également en droit d'attendre de leur part (art. 1 al. 2 LPol). L'action policière comprend l'activité de police administrative et de sécurité, ainsi que l'activité de police judiciaire, au sens de l'art. 15 du code de procédure pénale suisse du 5 octobre 2007 (CPP - RS 312.0), d'autre part (art. 1 al. 3 LPol).

Sauf dispositions légales contraires, la police est chargée des missions suivantes : assurer l'ordre, la sécurité et la tranquillité publics (let. a) ; prévenir la commission d'infractions et veiller au respect des lois, en particulier selon les priorités émises conjointement par le Conseil d'État et le Ministère public (let. b) ; exercer la police judiciaire (let. c) ; exécuter les décisions des autorités judiciaires et administratives (let. d) ; coordonner les préparatifs et la conduite opérationnelle en cas de situation exceptionnelle en vue de protéger la population, les infrastructures et les conditions d'existence (let. e) ; exercer les actes de police administrative qui ne sont pas dévolus à d'autres autorités (let. f ; art. 1 al. 4 LPol).

La conservation de données de géolocalisation des policiers lorsqu'ils sont en service se distingue de celle des images des caméras équipant les postes et locaux de la police judiciaire, durant 100 jours avant d'être détruites, laquelle est expressément prévue par l'art. 61 LPol (arrêt du Tribunal fédéral 1C_608/2016 du 18 mars 2017 consid. 3.4).

L'art. 31 LPol traite de la formation et du développement personnel au sein de la police, lesquels comptent parmi les obligations des policiers.

5.6 En l'occurrence, l'application vise à enregistrer les données de géolocalisation des policiers lorsqu'ils sont en service, soit en particulier « les identifiants de connexion (nom d'utilisateur/numéro de véhicule), les dates et heures (activation/désactivation), le terminal sur lequel l'application était activée, les coordonnées de géolocalisation relevées et le statut opérationnel » (art. 6.1 de la directive). Les données ainsi collectées permettent dès lors de retracer les trajets des policiers durant le laps de temps où ils sont en service.

Selon leur recommandation, les PPDT considèrent qu'il s'agit là de « données personnelles » au sens de la LIPAD, lesquelles ne sont toutefois pas constitutives de profils de personnalité des policiers. Les parties ne contestent pas ce point. Il est ainsi admis que les données traitées *in casu* concernent effectivement la sphère personnelle des policiers dans le cadre de leurs fonctions.

Au regard de ces éléments et de la jurisprudence susrappelée, l'utilisation de l'application par les policiers porte atteinte à leur sphère privée.

5.6.1 Les recourants considèrent que cette atteinte doit être qualifiée de grave.

Il ressort du dossier que depuis 2006, la majorité des véhicules de police était déjà équipée d'un système de géolocalisation, permettant de gérer et engager les

patrouilles de police sur le terrain. Par ailleurs, la directive ne prévoit pas un recours constant à l'application. Celle-ci est uniquement utilisée lorsque les policiers y sont connectés dans certaines situations spécifiques, conformément à la doctrine d'utilisation de l'application à l'annexe 1 de la directive (art. 5.2 de la directive).

L'utilisation de l'application est dès lors limitée à certaines tâches particulières des policiers pendant des périodes déterminées.

De même, la conservation des données de géolocalisation ainsi collectées est limitée à 100 jours (art. 6.5 de la directive).

Au vu de ce qui précède, l'atteinte aux droits personnels des policiers due à l'utilisation de l'application doit être qualifiée de limitée.

5.6.2 Le principe de géolocalisation des policiers n'est pas ancré dans une base légale formelle expresse, comme tel est le cas pour la vidéosurveillance. En revanche, l'art. 1 LPol mentionne les missions générales de la police, laquelle nécessite des moyens adéquats pour les remplir. L'art. 31 LPol ajoute l'obligation de formation et de développement personnel.

À cet égard, la directive dans sa version mise à jour au 14 juin 2023 indique, en préambule, que l'application est un complément du « système d'aide à l'engagement (ci-après : 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 » (art. 1 de la directive). Les objectifs de l'application 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 de l'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 des réquisitions ; porter secours ou engager des renforts au personnel de police en danger, accidenté ou se trouvant en difficulté lors d'une mission ou d'un engagement ; fournir des moyens de preuves utiles dans le cadre d'une procédure pénale ; analyser les données rétroactives 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 » (art. 2 de la directive).

Six des sept objectifs précités s'inscrivent dans la perspective des tâches de la police telles que définies aux art. 1 et 31 LPol, à savoir globalement assurer une gestion opérationnelle des ressources efficace en fournissant aux centrales les renseignements nécessaires à cette fin et permettre une consultation rétroactive des données à des fins de formation et d'amélioration du dispositif opérationnel.

En revanche, l'objectif ajouté après la mise à jour entrée en vigueur le 14 juin 2023, à savoir « fournir les moyens de preuves utiles dans le cadre d'une procédure pénale » (objectif n° 5) n'apparaît pas être en relation avec les missions de la police

définies à l'art. 1 LPol ni l'exigence de formation prévue à l'art. 31 LPol. Si, tel que rappelé précédemment, il existe une base légale expresse pour l'installation et l'utilisation de système de vidéosurveillance et la conservation des images filmées dans ce contexte, tel n'est pas le cas concernant l'enregistrement et l'utilisation des données de géolocalisation des policiers dans un autre but que pour remplir les missions générales de la police.

Ainsi que le relève le PPDT, l'ajout d'une finalité relative à la conservation de moyens de preuve potentiels en cas de dépôt de plainte pénale pourrait être invoquée dans n'importe quel contexte et pour toutes les données traitées par les institutions publiques.

Il s'ensuit que ce dernier objectif ne repose sur aucune base légale et devrait être supprimé pour ce seul motif, à l'exception des autres précités.

5.6.3 L'autorité intimée a justifié l'utilisation de l'application, avec tous les objectifs visés par son utilisation, par un intérêt public prépondérant au regard des missions de la police et de sa priorité du service à la population. S'agissant en particulier de l'objectif n° 5 de la directive, elle l'a appuyé par l'intérêt public prépondérant à établir les faits et l'intérêt privé prépondérant pour le policier visé par des plaintes pénales à pouvoir se disculper.

Les recourants et le PPDT ne contestent pas que l'utilisation de l'application afin de permettre la géolocalisation des policiers pour un engagement optimal des ressources policières sur le terrain constitue un intérêt public prépondérant. Ils discutent cependant la nécessité de conserver les données collectées dans ce contexte.

En effet, l'autorité intimée ne démontre pas en quoi la conservation des données de géolocalisation des policiers en service serait utile en cas de dépôt de plaintes pénales à leur encontre, dès lors qu'aucune information n'est transmise à ce sujet, hormis l'article de presse produit par les recourants. Celui-ci, relatant les propos de la commandante de la police, tend au contraire à prouver que le nombre de sanctions prononcées à l'encontre des policiers est faible proportionnellement au nombre total de plaintes pénales les visant. L'autorité intimée ne contredit d'ailleurs pas les chiffres indiqués.

À cela s'ajoute qu'en cas de réelle nécessité dans le cadre de l'instruction d'une plainte pénale, la position géographique d'un policier pourrait être déterminée par d'autres moyens techniques, applicables à tout justiciable. Conformément à la jurisprudence susrappelée, il ne se justifie pas dans ce contexte précis de faire une distinction entre un justiciable et un policier visé par une plainte pénale.

Par conséquent, sur ce point encore, l'objectif n° 5 n'apparaît pas justifié par un intérêt public prépondérant concret, tandis qu'il faut l'admettre pour les autres objectifs visés par la directive.

5.6.4 *In casu*, la question du respect du principe de la proportionnalité s'examine principalement sous l'angle de la durée de conservation des données de

géolocalisation des policiers, laquelle est problématique tant pour les recourants que pour le PPDT.

Dès lors qu'il faut retenir que celle-ci ne peut être motivée par la volonté de « fournir des moyens de preuves utiles dans le cadre d'une procédure pénale » (art. 2 de la directive), aucun des autres objectifs indiqués ne nécessite que lesdites données soient conservées durant une période de 100 jours, correspondant au délai de dépôt de plainte et de dix jours pour le délai d'envoi postal.

L'autorité intimée indique d'ailleurs disposer de 250 licences pour l'utilisation simultanée de l'application sans préciser si ce nombre serait suffisant à équiper l'ensemble des policiers devant intervenir, y compris en cas de grands événements. Cet élément tend à confirmer que le but principal de l'application est bel et bien d'assurer une localisation en temps réel des policiers sur le terrain afin d'améliorer l'efficacité des interventions.

Sous cet angle, un délai de conservation des données de géolocalisation supérieur à 24 heures n'apparaît pas proportionné aux buts poursuivis compte tenu de l'atteinte portée à la sphère personnelle des policiers dans le cadre de l'exercice de leurs fonctions.

Ainsi, si un délai de conservation des données de géolocalisation de 24 heures apparaît suffisant pour assurer le suivi opérationnel des interventions, rien ne justifie un délai de 100 jours.

Au vu des considérants qui précèdent, il y a lieu d'admettre les griefs des recourants quant à l'ajout de l'objectif n° 5, non pertinent, et au délai de conservation des données concernées de 100 jours, disproportionné. Ainsi, il appartiendra à l'autorité intimée de modifier la directive en ce sens que l'objectif n° 5 doit être supprimé, de même que le délai de conservation de 100 jours, lequel sera remplacé par un effacement automatique après 24 heures, conformément à la recommandation du PPDT. La décision du 8 juin 2023, seule objet du présent litige, sera annulée et le dossier renvoyé au département pour nouvelle décision dans le sens des considérants.

Par conséquent, le recours sera partiellement admis.

6. Vu l'issue du litige, aucun émolument ne sera perçu (art. 87 al. 1 LPA). Une indemnité de procédure de CHF 1'000.-, à charge de l'autorité intimée, sera allouée aux recourants, qui y ont conclu et ont eu recours aux services d'un avocat (art. 87 al. 2 LPA).

Le litige s'inscrit dans le contexte des rapports de service des recourants et des membres de la recourante. Il concerne toutefois une contestation non pécuniaire (art. 83 let. g de la loi fédérale sur le Tribunal fédéral du 17 juin 2005 – LTF - RS 173.110).

* * * * *

PAR CES MOTIFS

LA CHAMBRE ADMINISTRATIVE

à la forme :

déclare recevable le recours interjeté le 6 juillet 2023 par l'D_____, le C_____, A_____ et B_____ contre la décision du département des institutions et du numérique du 8 juin 2023 ;

au fond :

l'admet partiellement ;

annule la décision précitée dans le sens des considérants ;

renvoie la cause au département des institutions et du numérique pour nouvelle décision dans le sens des considérants ;

dit qu'il n'est pas perçu d'émolument ;

alloue une indemnité de procédure de CHF 1'000.- à l'D_____, le C_____, A_____ et B_____, solidairement entre eux, à la charge de l'État de Genève ;

dit que, conformément aux art. 82 ss de la loi fédérale sur le Tribunal fédéral du 17 juin 2005 (LTF - RS 173.110), le présent arrêt peut être portée dans les trente jours qui suivent sa notification par-devant le Tribunal fédéral, par la voie du recours constitutionnel subsidiaire, aux conditions posées par les art. 113 ss LTF ; le mémoire de recours doit indiquer les conclusions, motifs et moyens de preuve et porter la signature du recourant ou de son mandataire ; il doit être adressé au Tribunal fédéral, 1000 Lausanne 14, par voie postale ou par voie électronique aux conditions de l'art. 42 LTF. Le présent arrêt et les pièces en possession du recourant, invoquées comme moyens de preuve, doivent être joints à l'envoi ;

communique le présent arrêt à Mes Sylvain MÉTILLE et Marie-Laure PERCASSI, avocats des recourants, au département des institutions et du numérique, ainsi qu'au préposé cantonal à la protection des données et à la transparence.

Siégeant : Claudio MASCOTTO, président, Florence KRAUSKOPF, Francine PAYOT ZEN-RUFFINEN, Valérie LAUBER, Michèle PERNET, juges.

Au nom de la chambre administrative :

le greffier-juriste :	le président siégeant :
M. MAZZA	C. MASCOTTO

Copie conforme de cet arrêt a été communiquée aux parties.

Genève, le la greffière :