Requête en cessation d'un traitement de données illicite

Recommandation du 18 juillet 2023

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

1. Dans un courrier daté du 3 mai 2022 adressé à la Commandante de la Police cantonale genevoise, Me X a indiqué être mandaté par A, afin de défendre ses intérêts ainsi que ceux de ses membres.

2. Il s'est enquis de la base légale qui justifie l'enregistrement des appels reçus par la centrale d'engagement, de coordination et d'alarme (CECAL) et des communications transitant par le réseau radio POLYCOM, leur durée de conservation, les raisons pouvant justifier un accès et leurs modalités, ainsi que les mesures techniques et organisationnelles visant à assurer le respect des règles applicables à la sécurité des données. Il sollicitait copie de tous les documents en lien avec les demandes susmentionnées.

3. Le 28 juin 2022, la Commandante de la Police a répondu que l'enregistrement des appels téléphoniques reposait sur l'exception de l'art. 179^{quinquies} CP et que leur durée de conservation était de 12 mois. Les enregistrements étaient prévus pour des motifs probatoires, de formation, ainsi que de contrôle qualité. S'agissant de l'accès aux données hors procédure pénale, il était régi par la LCBVM et la LIPAD. Il n'y avait pas de documents spécifiques en la matière.

4. Par courrier du 15 juillet 2022, Me X s'est adressé à la responsable LIPAD départementale: le traitement des données à des fins probatoires, de formation et de contrôle qualité n'était pas des finalités reconnaissables, l'art. 179^{quinquies} CP ne constituait pas une base légale suffisante au traitement, la conservation des données personnelles pendant 12 mois était excessive et non conforme au principe de la proportionnalité. De plus, la personnalité des policiers était gravement atteinte par l'enregistrement systématique des conversations via le système radio POLYCOM. Me X terminait ainsi: « *en application des art. 37 et 39 LIPAD, des mesures doivent être prises pour mettre un terme à la conservation et au traitement illicite de données personnelles. On conclut dès lors à ce que les données ne soient pas conservées au-delà du strict nécessaire et uniquement dans le but de gérer les appels d'urgence. De manière générale, toute utilisation des données traitées par la CECAL (d'appels d'urgence et système radio POLYCOM) à des fins de surveillance des collaborateurs, de formation ou de contrôle qualité, doit être strictement interdite* ».

5. Le 20 janvier 2023, Me X et Me Y ont relancé la responsable LIPAD départementale.

6. Cette dernière a répondu par courrier du 20 février 2023 qu'un projet de loi sur l'information de police traitera de ces questions. Elle a ajouté que, dans la pratique actuelle, les données issues des enregistrements dont il est question ne sont utilisées que dans le cadre de procédures pénales et sur demande du Ministère public. L'utilisation à d'autres fins sera organisée lorsque les dispositions prévues dans le projet de loi sur l'information de police entreront en vigueur. La susnommée précise que les art. 35 al. 1 et 2 LIPAD, ainsi que l'art. 179^{quinquies} CP constituent des bases légales suffisantes, notant que, « *en l'espèce, il n'est pas établi que les données de conversations enregistrées constituent nécessairement des données personnelles*

sensibles. Le législateur n'exige pas une base légale formelle dans la mesure où l'intention du maître de fichier n'est pas de collecter des données personnelles sensibles. De la même manière, dans la mesure où ces données ne sont pas nécessairement sensibles par nature, l'on ne voit pas pourquoi il serait nécessaire de disposer d'une base légale formelle pour l'enregistrement des conversations téléphoniques ». La responsable LIPAD départementale ajoute que le principe de la proportionnalité est respecté, s'agissant de la conservation des données (art. 40 LIPAD) et que des mesures de sécurité sont existantes. Elle conclut que les données sont conservées pendant la durée que la police estime strictement nécessaire à l'accomplissement de ses missions, qu'aucune donnée n'est utilisée à des fins de surveillance des collaborateurs et que l'utilisation des données à des fins de formation et de contrôle qualité n'est pas mise en place tant que le police ne disposera pas d'une base légale formelle pour ce faire. Finalement, la qualité pour agir de A est mise en doute.

7. Par courrier du 2 mars 2023, Me X et Me Y ont sollicité que leur requête soit transmise au Préposé cantonal pour recommandation sur la question de la durée de conservation des données. S'agissant de la qualité pour agir de A, ils ont indiqué être au surplus mandatés par MM. B, C et D.

8. Le 8 juin 2023, Me X et Me Y ont relancé la responsable LIPAD départementale suite à leur courrier du 2 mars 2023.

9. Le 27 juin 2023, cette dernière a confirmé transmettre le dossier au Préposé cantonal.

10. 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:

11. 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.

12. 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.

13. 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 des institutions et du numérique (DIN) 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).

14. 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.

15. 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).

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. C'est en application des règles générales qu'il doit être déterminé si et dans quelle mesure les institutions publiques doivent détruire ou rendre anonymes les données qu'elles détiennent. Il n'a pas été jugé opportun de préciser dans la loi elle-même l'intervalle à partir duquel la destruction doit avoir lieu, ni de poser un critère univoque devant présider à la destruction des données, des règles générales en la matière n'étant guère concevables, tant elles sont étroitement liées à la diversité des tâches légales accomplies (MGC 2005-2006 X A 8503).

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.

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

19. En préambule, les Préposés relèvent qu'il a été donné une suite favorable à une partie des prétentions des requérants, de sorte que seule reste en suspens la question de la durée de conservation des enregistrements des conversations téléphoniques passant par la CECAL. Elle fait donc l'objet de la présente recommandation.

20. S'agissant des appels téléphoniques et radio passant par la CECAL, les Préposés retiennent qu'à ce jour, ils sont enregistrés à des fins probatoires. Les données issues desdits enregistrements ne sont utilisées que dans le cadre de procédures pénales et sur demande du Ministère public et sont conservées 12 mois, puis automatiquement détruites. Les requérants considèrent qu'une conservation de cette durée ne repose sur aucun fondement légal, est excessive et n'est ni nécessaire ni utile à atteindre les buts visés. Le DIN estime au contraire que la conservation des données intervient pour une durée strictement nécessaire à l'accomplissement des missions de la police.

21. Faute de disposition spécifique, l'art. 40 LIPAD prévoit que 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.

22. Comme mentionné ci-dessus, le législateur n'a pas souhaité préciser dans la loi elle-même l'intervalle à partir duquel la destruction doit avoir lieu, ni poser un critère univoque devant présider à la destruction des données. Il a considéré que des règles générales en la matière étaient peu concevables, tant la question est étroitement liée à la diversité des tâches légales accomplies (MGC 2005-2006 X A 8503). Dans le même sens, Philippe Meier note que « *la durée admise dépendra étroitement des finalités de la collecte et de la conservation, de la nature plus ou moins sensible (au sens technique) ou délicate (au sens non technique) des données et des impératifs de sécurité, puisque des risques accrus découlent d'une conservation longue durée* » (Philippe Meier, Protection des données, Berne, 2011, n°685).

23. Dès lors, la durée de conservation des données personnelles doit être déterminée au regard des missions légales de l'institution, des finalités pour lesquelles les données sont collectées et traitées, de leur nature ainsi qu'en application du principe de la proportionnalité.

24. Les missions de la police sont énumérées à l'art. 1 LPol: la police doit notamment assurer l'ordre, la sécurité et la tranquillité publics ou encore prévenir la commission d'infractions et veiller au respect des lois (art. 1 al. 4 litt. a et b LPol).

25. En particulier, la CECAL a pour mission principale « *d'assurer le trafic permanent des divers réseaux d'émission et de réception de messages radio, de transmettre aux ressources de police sur le terrain toutes les demandes ou réquisitions lui parvenant, notamment sur les numéros d'appels d'urgence 117 et 112 (appel d'urgence européen). Il s'agit d'un des centres névralgiques de la police genevoise. Dans son analyse des risques, la Cour des comptes a identifié la non-prise en charge adéquate d'un appel d'urgence (117 et 112), quel que soit son motif, comme un risque générique majeur »* (Rapport d'audit de gestion de la Cour des comptes relatif à la CECAL de la police genevoise: https://cdc-ge.ch/publications/audit-de-gestion-relatif-a-la-centrale-dengagement-de-coordination-et-dalarme-cecal-de-la-police-genevoise/).

26. En outre, les Préposés relèvent que le législateur fédéral, avec l'introduction de l'art. 179^{quinquies} al. 1 litt. a CP, qui n'est pas une base légale à un traitement de données personnelles, a voulu exclure le caractère punissable des enregistrements des conversations téléphoniques avec des services d'assistance, de secours ou de sécurité qui interviendraient sans le consentement des personnes concernées. Le message relatif à cette disposition indique que l'enregistrement systématique de ces appels sans avertissement préalable est en effet « *primordial pour assurer une intervention rapide et efficace et est en définitive également dans l'intérêt de la personne en situation de détresse* » (FF 1996 III 1411); lors d'une modification de cette disposition, le message l'accompagnant a précisé que « *les services d'assistance, de secours et de sécurité peuvent dès lors enregistrer en permanence leurs télécommunications* » (FF 2001 2508). L'art. 179^{quinquie}s al. 2 CP traite de l'utilisation des enregistrements en renvoyant aux art. 179bis al. 2 et 3 et 179ter al. 2. Selon la doctrine majoritaire, cela signifie que l'utilisation à des fins non autorisées d'enregistrements opérés en toute légalité est punissable. « *En d'autres termes, l'enregistrement ne doit être utilisé que pour vérifier l'origine de l'appel, identifier la personne en danger ou lutter contre les appels anonymes* » (CR CP II-Bichovsky, art. 179^{quinquies} CP, n°29). Le Préposé fédéral à la protection des données et à la transparence partage cette lecture (Document intitulé: « Conséquences pénales et civiles de l'enregistrement de conversations »: https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/arbeit_wirtschaft/audioueberwachung.html).

27. En l'espèce, il n'est plus contesté que l'enregistrement des appels téléphoniques et radio passant par la CECAL est nécessaire à l'accomplissement des tâches légales de

la police. Les enregistrements ne portent pas sur des données personnelles sensibles; leur finalité n'est pas de collecter de telles données. En conséquence, il n'est pas nécessaire d'élaborer une base légale spécifique. Il suffit, conformément aux art. 35 al. 1 et 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 et des missions de la CECAL. Les exigences de l'art. 35 LIPAD en matière de base légale sont donc respectées.

28. S'agissant du principe de finalité, les Préposés notent que le DIN a indiqué que les données issues des enregistrements ne sont utilisées qu'à des fins probatoires dans le cadre de procédures pénales et sur demande du Ministère public. Cette finalité est compatible avec les missions de la police décrites à l'art. 1 LPol, ce qui n'est plus contesté par les requérants.

29. La durée de la conservation des données doit ainsi être examinée, d'une part au regard des finalités pour lesquelles les enregistrements interviennent, à savoir vérifier l'origine de l'appel, identifier la personne en danger, lutter contre les appels anonymes et, sur demande du Ministère public, dans le cadre d'une procédure pénale, et d'autre part, au regard de l'importance de l'atteinte aux droits fondamentaux des personnes concernées.

30. Sous l'angle de la nécessité, la conservation des données pour vérifier l'origine de l'appel, identifier la personne en danger ou lutter contre les appels anonymes peut être de courte durée, quelques jours apparaissant suffisants. S'agissant des mesures probatoires (l'on peut imaginer une demande de la part du Ministère public d'enregistrements relatifs à une intervention suite à des violences conjugales par exemple, ou dans le cadre d'une plainte pénale pour menace), une durée de conservation très courte comporte le risque qu'en cas d'infraction découverte ultérieurement ou de dépôt d'une plainte pénale ultérieure, les enregistrements soient déjà effacés et qu'il ne soit plus possible d'y recourir comme moyen de preuve. Une certaine durée de conservation apparaît donc nécessaire.

31. Les Préposés relèvent, à titre exemplatif, que le Tribunal fédéral a considéré que la conservation d'images de vidéosurveillance du domaine public à des fins d'utilisation dans le cadre d'enquêtes pénales pour une durée de 100 jours était conforme à la Constitution et à la CEDH (ATF 133 I 77, cons. 5). En matière de vidéosurveillance, la LIPAD prévoit, à son art. 42 al. 2, une durée de conservation des images de 7 jours, délai qui peut être porté à 3 mois en cas d'atteinte avérée aux personnes et aux biens et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure. En matière de conservation de données secondaires de télécommunication, le Tribunal fédéral a relevé l'intérêt public important à leur utilisation dans le cadre d'enquêtes pénales et a considéré que, malgré l'importante atteinte aux droits fondamentaux, une conservation de 6 mois desdites données apparaissait proportionnée (ATF 144 I 126). Il sied de préciser que dans les cas de figure susmentionnés, la durée de conservation des données était prévue par la loi ou par un règlement.

32. En l'espèce, les enregistrements portent sur des communications avec la police ou les services de secours, communications initiées par la population. S'agissant des requérants, ils sont membres actifs de la police et ainsi pleinement informés des enregistrements des appels auxquels ils répondent. Les données traitées sont ainsi très circonscrites. En comparaison avec les jurisprudence susmentionnées, l'ingérence dans les droits fondamentaux des personnes concernées est bien moins significative dans le cas présent.

33. Au vu de ce qui précède, une conservation des enregistrements d'une durée de 3 mois apparaît acceptable au vu du délai pour déposer une plainte pénale. Par contre, une conservation des données durant 12 mois semble excessive et difficile à justifier sous l'angle de la nécessité. Les Préposés recommandent que la durée de conservation des enregistrements soit de 3 mois, à l'instar de ce que la LIPAD prévoit en matière de vidéosurveillance, et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure.

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande au Département des institutions et du numérique de limiter la durée de conservation des enregistrements de la CECAL à 3 mois sauf en cas de procédure pénale exigeant un délai de conservation plus long.

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

La présente recommandation est notifiée par pli recommandé à:

- Me X
- Mme, responsable LIPAD, Département des institutions et du numérique, Secrétariat général, Direction juridique, rue de l'Hôtel-de-Ville 14, Case postale 3952, 1211 Genève 3

Joséphine Boillat
Préposée adjointe

Stéphane Werly
Préposé cantonal

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.