Requête en cessation d'un traitement illicite

Recommandation du 15 mars 2024

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

1. Dans un courrier daté du 14 février 2024 adressé à la responsable LIPAD des Etablissements publics pour l'intégration (EPI), Me X a indiqué être mandaté par Mme Y (ci-après: la requérante). Il expliquait que sa mandante avait été convoquée à un entretien de service, "*pour deux raisons principales, soit une manipulation des timbrages dans l'application Mobatime et des consultations non autorisées de données personnelles sur l'application Vision RH*".

2. Il a indiqué que, s'agissant de Mobatime, les EPI avaient procédé à un croisement des données insérées manuellement par la requérante avec celles des relevés de l'utilisation de la clé électronique de la porte d'entrée. Me X a relevé que sa mandante n'avait jamais été informée que l'utilisation de sa clé était enregistrée à son nom et générait un fichier de données, ni n'y a donné son consentement. Par ailleurs, ces données étaient conservées à tout le moins pendant un an.

3. Il a ensuite expliqué que, concernant l'application Vision RH, il a été reproché à sa mandante d'avoir consulté des données personnelles de manière non autorisée, avec un audit à l'appui qui retraçait pendant plus d'un an toutes les personnes et recherches effectuées dans ce logiciel. Il indiquait que sa mandante n'avait jamais été informée que l'utilisation de ce logiciel générait un historique de ses recherches mentionnant la date et l'heure exacte, la page affichée, la personne, le caractère sensible de la donnée et le programme utilisé. Elle n'y avait en outre pas consenti, n'ayant pas signé la charte informatique et disant ne pas en avoir eu connaissance.

4. Me X a conclu son courrier en demandant à ce que le caractère illicite des traitements de données susmentionnés soit constaté, les principes de bonne foi et de reconnaissabilité de la collecte, de finalité et de proportionnalité n'étant pas respectés. Il a de surcroît sollicité la destruction des fichiers y relatifs concernant sa mandante.

5. Par courrier du 27 février 2024, la responsable LIPAD des EPI a saisi le Préposé cantonal, conformément à l'art. 49 al. 4 LIPAD, les EPI n'entendant pas faire intégralement droit aux prétentions de la requérante. Elle a indiqué que la requérante était une collaboratrice qui a fait l'objet d'une procédure administrative en raison de manquements à ses devoirs de fonction, à savoir la manipulation manuelle de ses timbrages et la consultation répétée et non-justifiée des données personnelles de tiers (ayant trait à la sphère privée et familiale de collaborateurs) au sein de l'application Vision RH. L'accès qui lui était octroyé pour cette dernière application relevait de ses fonctions au Service des ressources humaines.

6. Les EPI ont expliqué que les données au sujet desquelles la requérante se plaint d'un traitement illicite et pour lesquelles elle sollicite la destruction, ont été consultées et récoltées en raison de soupçons de manquements graves à ses devoirs de fonction qui ont été portés à la connaissance des EPI de manière fortuite, à savoir suite à des remontées de malversations. Ils ont encore précisé ce qui suit:

- L'application Vision RH (VRH) est une base de données utilisée par les Services des ressources humaines des EPI qui contient des données personnelles de l'ensemble des collaborateurs de l'institution (données d'état civil, parcours professionnel, informations contractuelles, données salariales, etc.), dont les accès sont limités à un usage strictement professionnel en lien avec les activités déployées par les collaborateurs des Services des ressources humaines. Cette base de données procède à des enregistrements automatiques des consultations et recherches effectuées par chaque profil utilisateur, qui sont conservées sur une période d'une année.

- L'accès au secteur où se situent les Services des ressources humaines n'est autorisé qu'à un nombre limité de collaborateurs, en raison du caractère confidentiel des activités qui s'y déploient et des dossiers qui s'y trouvent. Cet accès se fait au moyen d'une clé électronique qui doit être présentée à l'entrée pour générer son ouverture. La requérante dispose d'une telle clé avec accès à ce service où se situe son poste de travail. Une journalisation des ouvertures des portes sécurisées est générée automatiquement et enregistrée dans la base de données informatique. L'historique des accès est détruit après qu'une année se soit écoulée. Seule la direction des ressources humaines peut demander une extraction de cette journalisation en cas de soupçon de malversation d'un membre du personnel, ce qui est mentionné dans le document transmis pour signature aux collaborateurs lorsque la clé leur est remise. La requérante n'a pas signé ce document, car elle était déjà en fonction lorsqu'il a été mis en œuvre.

- Les EPI ont une charte informatique (cf. ci-dessous). Elle n'a pas été signée par la requérante, car elle a été instaurée après son entrée en fonction; toutefois, la mise en œuvre de ladite charte a été communiquée à tous les membres du personnel par courriel du 2 novembre 2020 et elle est librement accessible sur l'intranet de l'institution. De plus, la requérante a eu la charge de la transmettre aux nouveaux collaborateurs lorsqu'elle exerçait en qualité de gestionnaire RH.

7. Finalement, les EPI ont ajouté que la requête LIPAD dont il est question intervient dans le cadre d'une procédure administrative initiée par les EPI à l'encontre de la requérante. Ils considèrent que l'intérêt public à la manifestation de la vérité et au bon fonctionnement de l'institution – dans un contexte où la collaboratrice a procédé à des manipulations de ses timbrages au détriment de l'institution et qu'elle a violé ses obligations en matière de confidentialité en allant consulter un grand nombre de données personnelles dans le seul but de satisfaire sa curiosité personnelle – prime dans tous les cas tout éventuel intérêt privé à la destruction des pièces recueillies.

8. Ont été notamment remis au Préposé cantonal les extraits des consultations VRH, la Charte informatique des EPI (dont l'art. 9 sera repris ci-dessous), le courriel d'information du 2 novembre 2020 aux membres du personnel, et la quittance de remise de la clé électronique.

9. La quittance de remise de la clé électronique indique: "*Le membre du personnel est informé du fait que la clé électronique qui lui est remise est identifiée par un numéro qui lui est nominativement attribué. L'utilisation de cette clé donne lieu à une journalisation de ses accès aux différentes portes sécurisées. Ces données sont collectées à des fins de sécurité et conservées au sein de la base de données informatique "EXOS" gérée par les Services généraux et systèmes d'information des EPI. L'historique des accès est détruit après une année, et des extractions de cette journalisation peuvent être demandées au service précité par la direction des ressources humaines en cas de soupçon de malversation*".

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).

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

17. 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.

18. 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.

19. 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.

20. L'art. 64 al. 1 LIPAD prévoit que "*celui qui, au sein d'une institution soumise à la présente loi, traite des données personnelles à des fins étrangères à l'accomplissement des tâches légales qui lui sont confiées est passible de l'amende, sans préjudice des peines plus fortes prévues par le droit fédéral*". L'alinéa 4 ajoute que les contrevenants à la présente loi sont en outre passibles des sanctions disciplinaires prévues par leur statut spécifique.

21. Selon l'art. 43 al. 1 de la loi sur l'intégration des personnes handicapées du 16 mai 2023 (LIPH; RSGe K 1 36), les relations entre les EPI et son personnel sont régies par la législation cantonale relative au personnel de l'administration cantonale et des établissements publics médicaux (LPAC; RSGe B 5 05).

22. Le règlement d'application de la LPAC du 24 février 1999 (RPAC; RSGe B 5 05 01) prévoit à son art. 23A al. 4 que des contrôles statistiques et non individualisés de l'utilisation des ressources informatiques par le personnel peuvent être effectués. L'alinéa 5 dispose que "*lorsque les intérêts prépondérants de l'Etat de Genève, tels que la sécurité informatique ou le bon fonctionnement du service, l'exigent, des contrôles individualisés, et le cas échéant un accès à la liste des appels et à leur durée, au poste de travail informatique ou au compte de messagerie, peuvent être ordonnés par le chef du département ou son secrétaire général. Ces mesures respectent, dans toute la mesure du possible, la sphère privée des membres du personnel concernés*". Finalement, selon l'alinéa 6, le collège des secrétaires généraux précise par voie de directive l'utilisation de ces ressources par les membres du personnel et les mesures de contrôle y relatives.

23. La Charte informatique des EPI, qualifiée de directive à son art. 1, prévoit notamment:

    - art. 1, introduction : "*la présente directive régit l'utilisation des ressources informatiques mises à disposition des collaborateurs-trices et prévient les utilisations abusives. Elle informe officiellement les collaborateurs-trices que, pour des raisons d'exploitation, de sécurité et de contrôle, des enregistrements automatiques de données sont effectués régulièrement*".

    - Art. 9, mesures de contrôles:

        - 9.1.1 "*Différentes informations sont enregistrées de manière automatique, à savoir: le trafic de messagerie et d'internet, les données d'authentification, les accès aux serveurs de fichiers, les statistiques d'appels téléphoniques*.

        - 9.2.1 "*Des contrôles sont effectués régulièrement sur le contenu des volumes de stockages à savoir, la localisation du fichier, sa taille, son type, sa date de création et sa date de dernière modification*".

        - 9.3.1: "*Si un responsable hiérarchique dispose d'éléments concrets faisant soupçonner qu'un délit a été commis dans l'utilisation des ressources informatiques, il mandate le service des systèmes d'information afin que celui-ci réunisse les éventuelles preuves liées à la malversation. Il doit réunir les preuves matérielles (journaux, sauvegardes complètes et/ou partielles) qui, le cas échéant, seront remises aux autorités compétentes*."

- 9.3.2: "*Les autorités compétentes se chargent d'appliquer les éventuelles sanctions disciplinaires et décident si une plainte doit être déposée en cas d'abus*".

24. L'art. 26 al. 1 de l'Ordonnance 3 relative à la loi sur le travail du 18 août 1993 (OLT 3) prévoit qu'il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail; selon l'alinéa 2, "*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*".

25. Selon le commentaire de l'OLT 3, la protection de la personnalité des travailleurs, déjà ancrée dans l'art. 328b CO, s'étend par cet article au droit public du travail. Tant l'OLT 3 que les dispositions relatives à la protection des données personnelles ont pour but de garantir les droits fondamentaux des personnes et de protéger les travailleurs contre une surveillance de leur comportement. Le commentaire de l'OLT 3 relève qu'"*on entend par systèmes de surveillance ou de contrôle tous les systèmes techniques (optiques, acoustiques, électroniques, etc.) qui permettent d'enregistrer des données sur le comportement des travailleurs par des moyens techniques*"; tel est le cas par exemple des systèmes de logs d'application, mais pas les badges électroniques pour régler l'accès à une entreprise. Le commentaire précise que "*les systèmes et réseaux informatiques offrent de nombreuses possibilités de surveillance et de contrôle. L'entreprise doit informer au préalable leurs utilisateurs de la forme de surveillance employée pour les données concernant purement les affaires*".

26. Le commentaire de l'OLT 3 renvoie spécifiquement aux législations en matière de protection des données, s'agissant du traitement des données personnelles. Il rappelle les principes suivants: "*Le traitement de données personnelles obéit au principe de la bonne foi. La bonne foi signifie ici que le traitement des données doit être effectué de manière transparente pour la personne concernée, c'est-à-dire qu'elle est informée au préalable et de manière détaillée du type et du but du traitement. Le principe de la proportionnalité doit être systématiquement respecté. Il implique que seules les données pertinentes ou utiles doivent être traitées, puis effacées dans un laps de temps aussi court que possible, déterminé à l'avance. L'accès aux données personnelles traitées doit être réglementé à l'interne. Il doit être limité aux personnes habilitées à procéder à leur dépouillement. Après le contrôle, il est illicite d'archiver des données par souci de sécurité. L'emploi des technologies de l'information et de la communication, la saisie des données et leur dépouillement doivent être réglementés à l'interne. L'entreprise rédigera un règlement interne, dans lequel elle renseignera les travailleurs de manière transparente sur les droits et les obligations qui leur échoient dans le cadre de l'utilisation de systèmes de surveillance ou de contrôle (p. ex. installations téléphoniques, téléphonie sur internet et informatique) et sur la façon dont le contrôle et la surveillance internes à l'entreprise ont lieu*".

27. La Cour européenne des droits de l'Homme (CEDH) a rendu plusieurs arrêts en matière de surveillance des travailleurs, en application de l'art. 8 CEDH. Elle a rappelé la nécessité de l'existence d'une base légale (Affaire Copland contre Royaume-Uni du 3 avril 2007) et a reconnu l'atteinte à la vie privée du requérant dans une affaire où une entreprise avait surveillé ses communications électroniques et leur contenu. En effet, les juridictions nationales n'avaient pas vérifié si le requérant avait été préalablement averti par son employeur de la possibilité que ses communications soient surveillées et n'avaient pas non plus tenu compte du fait qu'il n'avait été informé ni de la nature ni de l'étendue de cette surveillance, ni du degré d'intrusion dans sa vie privée et sa correspondance. De surcroît, les juridictions nationales n'avaient pas déterminé, premièrement, quelles raisons spécifiques avaient justifié la mise en place des mesures

de surveillance, deuxièmement, si l'employeur aurait pu faire usage de mesures moins intrusives pour la vie privée et la correspondance du requérant et, troisièmement, si l'accès au contenu des communications avait été possible à son insu (Affaire Barbulescu contre Roumanie du 5 septembre 2017). Finalement, dans une affaire où des employées de supermarché avaient été mises sous vidéosurveillance, à leur insu, suite à des soupçons de vols, la Cour a conclu à la non-violation de l'art. 8 CEDH: un des arguments des requérantes était qu'elles n'avaient pas été averties au préalable de leur mise sous surveillance, malgré une obligation légale, mais la Cour a jugé qu'une telle mesure était clairement justifiée en raison des soupçons légitimes d'irrégularités graves et des pertes constatées, considérant l'étendue et les conséquences de cette mesure. En l'espèce, les tribunaux internes avaient donc conclu, sans outrepasser leur marge d'appréciation, que cette surveillance avait été proportionnée et légitime (Affaire Lopez Ribalda et autres contre Espagne du 17 octobre 2019).

28. Le Tribunal fédéral a rendu diverses jurisprudences qui précisent les contours de la surveillance admissible ou prohibée sur le lieu de travail. Dans un arrêt du 13 juillet 2004 (ATF 130 II 425), il a indiqué les conditions auxquelles l'adoption d'un dispositif impliquant une surveillance du comportement est autorisée: la surveillance doit être justifiée par un objectif légitime (impératifs de sécurité par exemple), le principe de la proportionnalité est respecté, et les travailleurs concernés ont préalablement été informés de son utilisation (consid. 4.4). L'hypothèse où la surveillance aurait pour but de vérifier un soupçon concret d'infraction et où une annonce préalable viderait la démarche de son sens est réservée (arrêt du Tribunal fédéral 9C_785/2010 du 10 juin 2011).

29. Dans un arrêt du 17 janvier 2013 (ATF 139 II 7), il a retenu que l'utilisation clandestine d'un logiciel espion était illicite et constituait une mesure prohibée par l'art. 26 al. 1 de l'OLT 3, en tant qu'elle est assimilable à un système de contrôle destiné essentiellement à surveiller le comportement d'un travailleur: dans le cadre de cette surveillance informatique, l'employeur avait pris connaissance et enregistré toutes les activités effectuées (et reproduites dans un rapport technique de 700 pages) par l'employé sur son ordinateur personnel entre le 15 juin et le 22 septembre 2009 et obtenu notamment des captures d'écran, c'est-à-dire des photographies de l'écran avec tout leur contenu.

30. Le Préposé fédéral à la protection des données s'est intéressé aux moyens techniques de surveillance sur le lieu de travail. Outre les grands principes qui sont mentionnés dans le commentaire de l'OLT 3, il a relevé notamment ce qui suit, concernant l'analyse de données secondaires : "*L'employeur doit respecter les dispositions réglant la protection des données lorsqu'il entend procéder à une analyse des données secondaires. Elle peut être effectuée sous forme anonyme, pseudonyme ou nominale. En vertu du principe de la proportionnalité, l'employeur doit toujours choisir la forme qui est appropriée pour le but visé (empêchement ou mise au jour d'abus) et constitue l'atteinte la moins importante aux droits de la personnalité de l'employé*"[1].

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

31. Conformément à l'art. 28 de la loi sur l'intégration des personnes handicapées (LIPH; RSGe K 1 36), les Etablissements publics pour l'intégration (EPI) sont un établissement

[1] https://www.edoeb.admin.ch/edoeb/fr/home/datenschutz/arbeit_wirtschaft/datenbearbeitung-arbeitgeber/technisch-mittel-ueberwachung-arbeitsplatz.html, consulté le 7 mars 2024.

de droit public, doté de la personnalité juridique et dont le siège est à Genève. De la sorte, la LIPAD leur est applicable (art. 3 al. 1 litt. c LIPAD).

32. La requérante, employée des EPI, fait valoir des prétentions en application de l'art. 47 al. 1 litt. b et c LIPAD, à savoir le constat et la cessation d'un traitement illicite de données personnelles la concernant, ainsi que la destruction des données ainsi collectées.

33. Le premier traitement illicite allégué a trait au croisement des données horaires insérées manuellement par la requérante dans l'application Mobatime avec celles issues des relevés de l'utilisation de sa clé électronique pour accéder au secteur du Service des ressources humaines. S'agissant de ce dernier relevé, la requérante a indiqué ne pas avoir été informée qu'un fichier était constitué.

34. En premier lieu, les Préposés relèvent que les données de journalisation étant liées à une personne identifiée, il s'agit d'un traitement de données personnelles au sens de la LIPAD.

35. Les Préposés ont pris note des éléments factuels suivants: la journalisation des ouvertures des portes sécurisées donnant accès au Service des ressources humaines est établie pour des raisons de sécurité, l'accès à ce secteur n'étant autorisé qu'à un certain nombre limité de collaborateurs, en raison du caractère confidentiel des activités qui s'y déploient et des dossiers qui s'y trouvent. L'extraction de la journalisation ne peut intervenir qu'en cas de soupçon de malversation. Lors de la remise de la clé, un document est signé par le membre du personnel, document qui l'informe de la journalisation et qu'une extraction de cette journalisation peut intervenir en cas de soupçon de malversation. La requérante n'a pas signé ce document, ayant pris ses fonctions avant qu'il ait été mis en œuvre.

36. Au regard des principes de protection des données, la journalisation issue de l'utilisation d'une clé électronique pour entrer dans un espace contenant des données confidentielles répond à l'exigence de la sécurité des données prévue par l'art. 37 LIPAD. Elle apparaît donc licite.

37. Le principe de la finalité du traitement implique que les données personnelles ne seront traitées que pour les buts annoncés au moment de leur collecte. En l'espèce, il apparaît que les données sont collectées à des fins de sécurité et qu'elles pourront être extraites en cas de soupçon de "malversation". A cet égard, les Préposés relèvent que le terme de "malversation" est peu précis et ne saurait se comprendre, dans le présent contexte, que comme une "malversation" en lien avec la sécurité des lieux, qui représente la finalité de la journalisation. Ils considèrent en conséquence que l'utilisation des données de journalisation liées à l'ouverture des portes à des fins de contrôle horaire correspond à une autre finalité que celle pour laquelle elle a été initialement prévue. En effet, la collecte de données en lien avec le contrôle horaire et son éventuel non-respect est un but tout différent de la collecte de données aux fins de garantir la sécurité des locaux. S'agissant de l'information donnée aux membres du personnel, selon laquelle les données pourront être extraites en cas de malversation, elle doit se comprendre, comme susmentionné, comme des malversations en termes d'accès indû aux locaux par exemple. Dès lors, l'utilisation de la base de données liées à la sécurité des locaux à des fins de contrôle horaire est contraire au principe de la finalité. Force est de constater que pour ce motif uniquement, le traitement est illicite.

38. S'agissant du principe de la bonne foi et de la reconnaissabilité de la collecte, il implique que le membre du personnel soit informé de ladite collecte, ce qui est le cas pour les collaborateurs et collaboratrices ayant signé la quittance de remise de la clé et

s'agissant de la journalisation à des fins de sécurité. L'utilisation des données de journalisation à des fins de contrôle horaires n'est ne revanche pas reconnaissable pour les motifs mentionnés au point 37. Le principe de la reconnaissabilité n'est ainsi pas respecté.

39. La question se pose de savoir si, en raison des soupçons pesant sur la requérante et qui ont conduit au croisement des deux fichiers de données, le traitement de données était admissible. Les Préposés considèrent que tel n'est pas le cas. En effet, le principe de la proportionnalité exige que les mesures les moins attentatoires soient adoptées pour atteindre le but poursuivi. En l'espèce, l'employeur pouvait constater la manipulation des horaires par un autre biais (surveillance directe du supérieur hiérarchique par exemple).

40. Au vu de ce qui précède, les Préposés considèrent que l'utilisation de la journalisation relative à la clé d'ouverture des portes sécurisées à des fins de contrôle horaire constitue un traitement illicite, auquel les EPI doivent mettre fin. Conformément à l'art. 47 al. 1 litt. b LIPAD, les effets doivent en être supprimés.

41. Le second traitement illicite allégué a trait à la journalisation des recherches de la requérante dans l'application VRH et à son extraction, qui a conduit au constat qu'elle avait consulté de nombreuses informations sur des membres du personnel, alors qu'elle n'en avait pas le besoin dans le cadre de ses fonctions.

42. Les EPI ont indiqué que le système de journalisation intervenait pour des questions de sécurité des données, la base de données VRH contenant de nombreuses données personnelles, y compris sensibles, des membres du personnel. La conservation des données de journalisation est d'un an.

43. Comme mentionné ci-dessus, les données de journalisation étant liées à une personne identifiée, il s'agit d'un traitement de données personnelles au sens de la LIPAD. Les Préposés notent en outre qu'un système de contrôle des logs relève d'une mesure de surveillance au sens de l'OLT 3.

44. S'agissant du principe de la légalité, les Préposés relèvent que, conformément à l'art. 35 LIPAD, 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. L'art. 37 al. 1 LIPAD prévoit que les données personnelles doivent être protégées contre tout traitement illicite par des mesures organisationnelles et techniques appropriées. Selon l'art. 23A al. 5 RPAC, lorsque les intérêts prépondérants de l'Etat l'exigent (tels la sécurité informatique et le bon fonctionnement du service), des contrôles individualisés peuvent être ordonnés. La Charte informatique des EPI prévoit à son art. 9.3.1 que si un responsable hiérarchique dispose d'éléments concrets faisant soupçonner qu'un délit a été commis dans l'utilisation des ressources informatiques, il mandate le service des systèmes d'information afin que celui-ci réunisse les éventuelles preuves liées à la malversation.

45. S'agissant des mesures de surveillance sur le lieu de travail, le Tribunal fédéral a indiqué les conditions auxquelles l'adoption d'un dispositif impliquant une surveillance du comportement est autorisée: la surveillance doit être justifiée par un objectif légitime (impératifs de sécurité par exemple), le principe de la proportionnalité est respecté, et les travailleurs concernés ont préalablement été informés de son utilisation.

46. En l'espèce, les Préposés considèrent que les conditions susmentionnées sont respectées. En effet, le principe de la journalisation des logs à des fins de protection des données personnelles repose sur une base légale suffisante. En tant que dispositif

de surveillance, il est justifié par un objectif légitime qui est la protection de la sphère privée des membres du personnel et la sécurité de leurs données. Le principe de la proportionnalité est respecté dans la mesure où une extraction des données de journalisation n'intervient qu'en cas de soupçons d'utilisation abusive; de plus, l'on ne voit pas par quel moyen moins intrusif l'objectif légitime précité pourrait être sauvegardé. Finalement, les membres du personnel ont été informés des possibilités de contrôle, que ce soit par les bases légales existantes ou la Charte informatique des EPI. Le principe de la légalité est ainsi respecté.

47. S'agissant de la reconnaissabilité de la collecte, la requérante allègue ne pas avoir eu connaissance de la Charte informatique, ni de son contenu. Les Préposés considèrent qu'elle ne saurait être suivie sur ce point. En effet, bien que la requérante n'ait pas signé ladite charte, elle lui a été communiquée par courriel, comme à l'ensemble du personnel. De plus, de par sa fonction au sein des ressources humaines, elle a été amenée à la faire signer à d'autres. Ainsi, il sied de retenir que la requérante avait été informée de l'existence de la Charte informatique et de son contenu.

48. Au regard de la finalité du traitement, les Préposés relèvent que l'extraction de la journalisation est intervenue suite à des soupçons d'utilisation abusive de l'application. L'extraction contestée répond ainsi à la finalité pour laquelle la journalisation a été mise en place, de sorte que le principe de finalité est respecté.

49. S'agissant du principe de la proportionnalité, comme mentionné ci-dessus, il sied de retenir qu'il a été respecté dans la mesure où une extraction des données de journalisation n'intervient qu'en cas de soupçons d'utilisation abusive; l'on ne voit pas quel moyen moins intrusif permettrait de sauvegarder l'intérêt légitime de la protection de la sphère privée des membres du personnel de la consultation abusive de leurs données. La durée de conservation des données de journalisation pendant un an ne paraît pas disproportionnée.

50. Au vu de ce qui précède, les Préposés considèrent que la journalisation des accès dans l'application VRH est conforme à la LIPAD.

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande aux Etablissements publics pour l'intégration :

- De constater que l'utilisation de la journalisation relative à la clé d'ouverture des portes sécurisées du Service des ressources humaines à des fins de contrôle horaire constitue un traitement illicite et d'y mettre fin.
- De constater que la journalisation des accès dans l'application VRH est conforme à la LIPAD.

Dans les 10 jours à compter de la réception de la présente recommandation, les Etablissements publics pour l'intégration doivent rendre une décision sur les prétentions de la requérante (art. 49 al. 6 LIPAD).

La présente recommandation est notifiée par pli recommandé à:

- Me X
- Mme A, responsable LIPAD, Etablissements publics pour l'intégration, Direction générale, route de Chêne 48, 1208 Genève

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.