RÉPUBLIQUE ET CANTON DE GENÈVE

POST TENEBRAS LUX

POUVOIR JUDICIAIRE

A/1536/2024-LIPAD **ATA/1316/2024**

COUR DE JUSTICE

Chambre administrative

Arrêt du 12 novembre 2024

dans la cause

A_____ **recourante**
représentée par Me Yann LAM, avocat

contre

ÉTABLISSEMENTS PUBLICS POUR L'INTÉGRATION (EPI) **intimés**
représentés par Me Sébastien VOEGELI, avocat

et

PRÉPOSÉ CANTONAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE **appelé en cause**

_____

EN FAIT

A. **a.** A_____ était collaboratrice au sein des Établissements publics médicaux (ci-après : EPI) du 1er janvier 2008 au 23 février 2024.

b. Elle travaillait en qualité de gestionnaire des ressources humaines (ci- après : RH), chargée de la formation.

B. **a.** Le 9 janvier 2024, en raison de soupçons de sa hiérarchie en lien avec ses horaires, les EPI ont extrait les données concernant ses entrées au moyen de sa clé électronique dans les locaux sis au __ étage du bâtiment où elle travaillait, sis route B_____ (service C_____), pendant la période du 16 janvier 2023 au 4 janvier 2024. Ils ont croisé ce fichier de données avec les entrées manuelles des horaires de la collaboratrice dans l'application officielle dédiée à l'enregistrement du temps de travail des membres du personnel, MOBATIME.

Une seconde extraction des données a été réalisée le 11 janvier 2024 concernant les recherches et consultations de données personnelles effectuées dans la base de données Vision RH (ci-après : VRH) par la collaboratrice afin d'établir l'existence ou non d'un manquement à ses obligations professionnelles et son étendue.

b. Ces deux fichiers contenaient des données personnelles de la collaboratrice, notamment ses noms et prénoms ainsi que les données de consultations des applications.

c. Le 15 janvier 2024 s'est tenu un entretien de service, au cours duquel la hiérarchie a reproché à A_____ une manipulation des timbrages dans l'application MOBATIME et des consultations non autorisées de données sur l'application VRH. Elle a appris à cette occasion que des données la concernant avait été récoltées durant une année.

d. Le 22 février 2024, une décision de résiliation des rapports de service avec effet immédiat a été notifiée à A_____ par les EPI en raison de soupçons de manquements graves à ses devoirs de fonction, découverts fortuitement les 4 et 11 janvier 2024 en lien avec des manipulations de timbrages et des consultations non autorisées de données personnelles de collaborateurs de l'institution dans l'application VRH.

Son licenciement se fondait sur les fichiers obtenus dans le cadre des extractions de VRH et de la journalisation relative à l'utilisation de sa clé électronique pour ouvrir les portes sécurisées du 1er étage. Les manquements ainsi constatés étaient suffisants pour mettre fin aux rapports de service de leur collaboratrice avec effet immédiat.

e. Le 21 mars 2024, A_____ a interjeté recours à l'encontre de cette décision (procédure A/981/2024) auprès de la chambre administrative de la Cour de justice (ci-après : la chambre administrative).

C. **a.** Le 14 février 2024, A_____ a formulé une requête auprès de son employeur en constat du caractère illicite du traitement de ses données personnelles en lien avec les deux extractions citées sous let. B.a. Ces éléments devaient être détruits conformément à l'art. 47 al. 1 let. b et c de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles du 5 octobre 2001 (LIPAD - A 2 08).

b. Le 27 février 2024, cette requête a été transmise au préposé cantonal à la protection des données (ci-après : le préposé) par les EPI, afin qu'il leur adresse une recommandation sur la suite à lui donner.

c. Dans sa recommandation du 15 mars 2024, le préposé a considéré que la journalisation des accès dans l'application VRH était conforme à la LIPAD et ne constituait pas un traitement illicite des données personnelles de la collaboratrice. En revanche, l'utilisation à des fins de contrôle horaire de la journalisation des données de la collaboratrice relative aux ouvertures des portes sécurisées du service C_____ au moyen de sa clé électronique constituait un traitement illicite de ses données. Il s'agissait d'y mettre fin. Les principes de finalité et de reconnaissabilité n'étaient pas respectés, car la notion indiquée dans les quittances de remise des clés « en cas de soupçon de malversation » ne pouvait se comprendre qu'en lien avec la sécurité des lieux (accès indu aux locaux) et non en lien avec un contrôle horaire. Le préposé estimait en outre que le principe de proportionnalité n'était pas respecté en l'espèce, au motif que l'employeur aurait pu constater la manipulation alléguée des horaires d'une autre manière, par exemple par la surveillance directe du supérieur hiérarchique.

D. **a.** Par décision déclarée exécutoire nonobstant recours du 28 mars 2024, les EPI ont constaté que la journalisation des accès dans l'application VRH (ch. 1) et celle relative à la clé d'ouverture des portes sécurisées du service RH (ch. 2) étaient conformes à la LIPAD. Ils considéraient que l'utilisation de la journalisation précitée à des fins de contrôle des horaires de travail dans le contexte de la procédure administrative A/981/2024 était ainsi licite (ch. 3). Ils ont refusé de procéder à la destruction des fichiers générés par les deux extractions querellées aussi longtemps que la procédure de recours A/981/2024 était pendante (ch. 4).

Ils suivaient la recommandation du préposé au sujet de la journalisation des accès dans l'application VRH. En revanche, leur position divergeait de l'interprétation du préposé s'agissant de la notion de « soupçons de malversation » figurant sur la quittance de remise de la clé électronique. Ces termes ne leur permettaient pas uniquement de procéder à une extraction de cette journalisation en cas de problèmes liés à la sécurité des lieux mais également en cas de problématiques liées à la gestion du personnel comme celles visées dans la procédure administrative concernant la collaboratrice. Le but de la collecte des données, soit le contrôle des horaires de travail et la possibilité d'extraire les données correspondantes, était reconnaissable, en particulier par le fait que la directrice RH était nommée comme disposant de la

faculté de demander ces extractions en cas de soupçons de malversations par un collaborateur.

Il n'existait pas de mesure plus proportionnée, telle qu'une surveillance hiérarchique pour ce type particulier de résiliation, au regard des exigences légales en matière de rapidité de réaction qu'imposaient ces décisions.

Enfin, dans la mesure où la collaboratrice avait interjeté recours le 21 mars 2024 à l'encontre de la décision de résiliation de ses rapports de service (procédure A/981/2024), il n'y avait pas lieu de procéder à la destruction des fichiers générés par les extractions querellées dans la mesure où ils constituaient des moyens de preuve faisant partie intégrante du dossier de recours.

b. Par acte du 6 mai 2024, A_____ a interjeté recours devant la chambre administrative contre la décision précitée, concluant à l'annulation des points 2 à 4 de cette décision et au constat que l'utilisation de la journalisation relative à la clé d'ouverture des portes sécurisées du service C_____ à des fins de contrôle horaire constituait un traitement illicite de ses données. Celles-ci devaient être détruites.

À titre liminaire, elle soulignait que la question du traitement des données liées à l'utilisation de l'application VRH, considéré comme licite par le préposé, n'était pas contestée.

La journalisation et l'extraction des données liées à l'utilisation de la clé d'ouverture des portes n'était pas un moyen fiable permettant de procéder à un contrôle horaire. Cette clé ne permettait que d'ouvrir la porte depuis l'extérieur, alors que le départ de la zone sécurisée ne nécessitait pas de badger, la porte étant automatique. Si l'autorité intimée souhaitait utiliser ce moyen comme contrôle auxiliaire, outre la pointeuse, elle aurait dû installer un système nécessitant de pointer aussi pour quitter la zone sécurisée.

La récolte de telles données n'atteignait pas son but. Le préposé avait estimé à juste titre que le principe de finalité avait été violé. En outre, les principes d'information et de reconnaissabilité avaient été violés. Elle n'avait jamais signé la quittance de remise des clés et le fait que la directrice RH soit mentionnée comme pouvant ordonner une telle extraction ne pouvait être interprété comme un élément permettant de reconnaitre le but de la collecte des données. Le principe de proportionnalité n'était pas respecté non plus, dès lors que l'autorité aurait pu prendre le temps de faire son enquête, la rapidité de réaction attendue aux fins d'un licenciement immédiat requise par la jurisprudence ne s'appliquant qu'entre le moment où les faits de nature à rompre les liens de confiance étaient découverts et la décision qui s'ensuivait. Le litige ne portait pas sur la question de la validité du licenciement immédiat mais bien sur l'enquête qu'aurait dû effectuer l'employeur. Enfin, en prétendant qu'il était exclu de procéder à une destruction des fichiers servant de moyens de preuve dans le cadre d'une procédure pendante à la chambre administrative, les EPI se méprenaient, l'existence d'une telle procédure ne présupposant pas un droit de l'autorité intimée à violer la loi, en particulier celle

liée à la protection des données. Admettre cette hypothèse revenait à avantager la partie violant la loi, ce qui n'était pas admis d'une autorité administrative, l'abus de droit ne méritant aucune protection.

c. Dans leurs observations du 21 mai 2024, le préposé et la préposée adjointe ont maintenu leur position exprimée dans la recommandation du 15 mars 2024. Le traitement des données querellées avait trait au croisement des données horaires insérées manuellement par la recourante dans l'application MOBATIME avec celles issues des relevés de l'utilisation de sa clé électronique pour accéder au secteur du service C_____. Comme déjà exprimé, le traitement ne respectait pas le principe de la finalité de la collecte, la journalisation de l'ouverture des portes intervenant à des fins de sécurité et non de contrôle horaire. Il était recommandé aux EPI d'y mettre fin et d'en supprimer les effets, conformément à l'art. 47 al. 1 let. b LIPAD. Sur ce point, leur recommandation n'avait pas été suivie par les EPI.

d. Dans leurs observations du 8 juillet 2024, les EPI ont conclu au rejet du recours.

La procédure s'inscrivait dans un rapport étroit de connexité avec la cause A/981/2024. Ils avaient déjà pris position de manière détaillée sur le reproche qui leur était adressé de traitement illicite des données dans le cadre de leurs observations du 22 avril 2024 dans cette cause.

Le traitement respectait le principe de finalité, contrairement à l'avis du préposé. La définition du terme « malversation » allait dans le sens d'un comportement humain répréhensible, cela au sens du droit pénal ou du droit administratif. Le terme de malversation n'était pas limité à la sécurité des lieux, comme le soutenait le préposé. Cette interprétation était corroborée par la mention du terme malversation dans le paragraphe consacré aux actes illicites de la charte informatique des EPI. Elle l'était également dans la quittance de remise de la clé électronique. Le timbrage inexact au détriment de l'employeur constituait une grave violation du devoir de fidélité du travailleur, justifiant son renvoi immédiat. L'acte de timbrer inexactement ses horaires de travail était « à l'évidence englobé dans la définition du terme de malversation ». Le principe de finalité n'avait pas été violé : le traitement des données avait été effectué dans les limites du cadre annoncé, à savoir la prévention et l'investigation de comportements potentiellement illicites de la part des porteurs de badges.

Le principe de reconnaissabilité avait également été respecté, tout porteur de badge étant informé que la journalisation de ses accès serait utilisée pour élucider des soupçons de malversation.

Enfin, le principe de proportionnalité avait été respecté, la solution proposée par le préposé n'étant ni praticable ni souhaitable. Au titre de la surveillance des employés, le SECO préconisait par exemple un contrôle ponctuel effectué par badge au lieu d'une surveillance permanente. La solution mise en place par les EPI, à savoir de croiser les données d'accès à la porte avec les entrées dans MOBATIME était proportionnée car étant moins intrusive qu'une surveillance de la recourante

par sa hiérarchie. Ils avaient ainsi ménagé le principe de proportionnalité en choisissant la solution la moins intrusive possible.

e. Dans sa réplique du 22 août 2024, la recourante a rappelé ne jamais avoir été chargée de remettre les clés et badges aux utilisateurs, de sorte qu'elle ne savait pas que la journalisation des accès était enregistrée et pouvait être exploitée, comme la quittance de remise des médias utilisateurs le précisait.

Le principe de reconnaissabilité n'avait pas été respecté. Elle n'avait jamais été informée que des données étaient récoltées lors de l'ouverture de la porte avec un badge. Il n'était enfin pas nécessaire de badger pour sortir du secteur, rendant un contrôle horaire *de facto* impossible. Enfin, elle bénéficiait d'un horaire variable et il aurait donc fallu en toute cohérence disposer d'un contrôle de sortie pour reconstituer un horaire. Sous l'angle de l'aptitude, le moyen ne permettait pas d'atteindre les buts fixés par l'employeur, violant le principe de la proportionnalité. L'exploitation des données ainsi récoltées en vue du contrôle horaire était illicite.

f. Sur ce, les parties ont été informées que la cause était gardée à juger.

EN DROIT

1. Interjeté en temps utile devant la juridiction compétente, le recours est recevable (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. Il y a lieu préalablement de préciser l'objet du litige.

2.1 L'objet du litige est principalement défini par l'objet du recours (ou objet de la contestation), les conclusions du recourant et, accessoirement, par les griefs ou motifs qu'il invoque. L'objet du litige correspond objectivement à l'objet de la décision attaquée, qui délimite son cadre matériel admissible (ATF 136 V 362 consid. 3.4 et 4.2 ; arrêt du Tribunal fédéral 2C_581/2010 du 28 mars 2011 consid. 1.5 ; ATA/499/2021 du 11 mai 2021 consid. 2a). La contestation ne peut excéder l'objet de la décision attaquée, c'est-à-dire les prétentions ou les rapports juridiques sur lesquels l'autorité inférieure s'est prononcée ou aurait dû se prononcer. L'objet d'une procédure administrative ne peut donc pas s'étendre ou qualitativement se modifier au fil des instances, mais peut tout au plus se réduire dans la mesure où certains éléments de la décision attaquée ne sont plus contestés. Ainsi, si un recourant est libre de contester tout ou partie de la décision attaquée, il ne peut pas prendre, dans son mémoire de recours, des conclusions qui sortent du cadre des questions traitées dans la procédure antérieure (ATA/499/2021 du 11 mai 2021 consid. 2a).

2.2 En l'espèce, l'objet du litige est limité aux points 2 à 4 de la décision des EPI du 28 mars 2024, soit le constat par ces derniers de la conformité à la LIPAD de la journalisation des données relatives à la clé d'ouverture des portes sécurisées,

l'utilisation considérée comme licite de ces données à des fins de contrôle des horaires de travail dans le contexte de la procédure administrative à l'encontre de la recourante et leur refus de détruire ces données.

La question de la journalisation des accès dans l'application VRH n'est plus litigieuse, la recourante ayant admis la position du préposé, lequel estimait que le traitement de ces données était licite et proportionné.

3. La recourante souhaite le constat de l'illicéité du traitement des données issues de la journalisation de ses entrées au moyen de la clé électronique ainsi que la destruction des fichiers correspondants.

3.1 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 et, 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). Elle comporte ainsi deux volets, l'un concernant l'information du public et l'accès aux documents réglé dans le titre II (art. 5 ss LIPAD), qui n'est pas en cause dans le cadre du présent recours, et l'autre portant sur la protection des données personnelles, dont la réglementation est prévue au titre III (art. 35 ss LIPAD).

3.2 Elle s'applique notamment aux institutions, établissements et corporations de droit public cantonaux et communaux, ainsi que leurs administrations et les commissions qui en dépendent (art. 3 al. 1 let. c LIPAD).

3.3 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). Selon l'art. 4 let. b LIPAD, par données personnelles sensibles, on entend les données personnelles sur la sphère intime (ch. 2) et des poursuites ou sanctions pénales ou administratives (ch. 4).

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).

3.4 Selon 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 (al. 1). 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 (al. 2).

3.5 L'art. 36 al. 1 LIPAD dispose 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) ainsi qu'exactes et si

nécessaire mises à jour et complétées, autant que les circonstances permettent de l'exiger (let. b). 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).

3.6 La collecte de données personnelles doit être faite de manière reconnaissable pour la personne concernée (art. 38 al. 1 LIPAD).

3.7 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).

3.8 L'art. 47 al. 1 LIPAD prévoit que toute personne physique ou morale de droit privé peut notamment, 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) ou constatent le caractère illicite du traitement (al. 3).

Sauf disposition légale contraire, elle est en particulier en droit d'obtenir des institutions publiques, à propos des données la concernant, qu'elles détruisent celles qui ne sont pas pertinentes ou nécessaires (al. 2 let. a), qu'elles rectifient, complètent ou mettent à jour celles qui sont respectivement inexactes, incomplètes ou dépassées (al. 2 let. b).

3.9 Selon l'art. 49 LIPAD, toute requête fondée sur l'art. 47 LIPAD notamment doit être adressée par écrit au responsable chargé de la surveillance de l'organe dont relève le traitement considéré (al. 1). Si le responsable 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 avec ses observations et les pièces utiles (al. 2). 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 (al. 3). L'institution concernée statue alors par voie de décision dans les dix jours sur les prétentions du requérant (al. 4).

À cet égard, la chambre de céans a d'ores et déjà jugé que l'absence d'une recommandation préalable du préposé ne pouvait conduire à une irrecevabilité du recours contre la décision querellée mais plutôt à son annulation pour violation d'une règle essentielle de procédure (ATA/229/2018 du 13 mars 2018 consid. 6 d).

3.10 En droit privé, l'art. 328b de la loi fédérale du 30 mars 1911, complétant le Code civil suisse (CO, Code des obligations - RS 220), prévoit que l'employeur ne

peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale sur la protection des données du 19 juin 1992 (LPD - RS 235.1) sont applicables. Cet article règlemente les questions liées à la protection des données dans le contrat de travail (Marie MAJOR, Questions spécifiques/Le droit d'accès de l'employé à son dossier personnel ; *in* Jean-Philippe DUNAND/Pascal MAHON [éd.], La protection des données dans les relations de travail, 2017, p. 289).

À l'instar de ce qui prévaut pour l'art. 328 CO, l'art. 328b CO doit également s'appliquer par analogie en droit public, en l'absence de dispositions expresses prévues par le droit de la fonction publique (ATA/649/2023 du 20 juin 2023 consid. 2.3.2.3 et les références citées).

3.11 L'art. 26 al. 1 de l'ordonnance 3 relative à la loi fédérale sur le travail dans l'industrie, l'artisanat et le commerce du 13 mars 1964 (LTr - RS 822.11) (ci-après : OLT 3) concerne la surveillance des travailleurs. La protection de la personnalité des travailleurs, ancrée à l'art. 328 CO, qui s'étend par cet article au droit public du travail, rappelle que le traitement des données personnelles doit respecter le principe de la bonne foi. Dans ce cadre, cela signifie que le traitement des données doit être effectué de manière transparente pour la personne concernée, c'est-à-dire qu'elle doit être informée au préalable de manière détaillée du type et du but du traitement. Le principe de proportionnalité doit être systématiquement respecté (Commentaire de l'OLT 3 du Secrétariat d'État à l'économie *ad* art. 26 p. 6).

3.12 Les relations entre les EPI et son personnel sont régies par 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. 43 al. 1 de la loi sur l'intégration des personnes handicapées du 16 mai 2003 - LIPH - K 1 36). Des contrôles statistiques et non individualisés de l'utilisation des ressources informatiques par le personnel peuvent être effectués (art. 23A al. 4 du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux du 24 février 1999 - RPAC - B 5 05.01). Lorsque les intérêts prépondérants de l'État 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, 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 tout la mesure du possible la sphère privée des membres du personnel concernés (art. 23A al. 5 RPAC).

3.13 Les directives sont des ordonnances administratives dont les destinataires sont ceux qui sont chargés de l'exécution d'une tâche publique, et non les administrés. Elles ne sont pas publiées dans le recueil officiel de la collectivité publique et ne peuvent donc avoir pour objet la situation juridique de tiers

(Pierre MOOR/Alexandre FLÜCKIGER/Vincent MARTENET, Droit administratif, vol. I, 3e éd., 2012, ch. 2.8.3.1). Une ordonnance administrative ne lie pas le juge, mais celui-ci la prendra en considération, surtout si elle concerne des questions d'ordre technique, tout en s'en écartant dès qu'il considère que l'interprétation qu'elle donne n'est pas conforme à la loi ou à des principes généraux (arrêt du Tribunal fédéral 2C_348/2022 du 7 mars 2023 ; ATA/697/2016 du 23 août 2016 consid. 5c ; ATA/722/2015 du 14 juillet 2015 consid. 4b ; ATA/31/2012 du 17 janvier 2012 consid. 7).

3.14 La charte informatique des EPI (ci-après : la charte informatique) est, comme le rappelle son al. 1, une directive. Elle précise à son art. 9 les mesures de contrôles possibles. Notamment, différentes informations peuvent être enregistrées de manière automatique à savoir : le trafic de messagerie et d'internet, les données d'authentification, les accès aux serveurs de fichiers et les statistiques d'appels téléphonique (ch. 9.1.1). 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 (ch. 9.3.1).

La quittance de remise des « médias utilisateurs » des EPI précise que : « 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 donnée 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. ».

3.15 En l'espèce, les EPI considèrent que la journalisation des données liées à l'utilisation de la clé est conforme à la LIPAD et refusent donc sa destruction. Les termes utilisés dans la charte informatique étaient clairs et couvraient également la question du timbrage.

Le préposé a retenu que tel n'était pas le cas, faute pour l'usage des données d'être conforme aux principes de la finalité, de reconnaissabilité et de proportionnalité. La recourante souscrit à l'avis de ce dernier.

À titre préalable, il sera rappelé que les EPI sont un établissement public, doté de la personnalité juridique et dont le siège est à Genève (art. 28 LIPH). La LIPAD leur est applicable (art. 3 al. 1 let. c LIPAD).

Il n'est pas querellé que les données journalisées sont liées à une personne identifiée et qu'il s'agit ainsi d'un traitement des données personnelles au sens de la LIPAD. La chambre de céans ne peut que suivre l'avis du préposé relatif au traitement illicite du croisement des données horaires insérées manuellement par la recourante dans MOBATIME et celles issues de relevés de l'utilisation de sa clé électronique

pour accéder au service RH. En effet, selon le préposé, le principe de finalité (art. 35 al. 1 LIPAD) implique que 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 pas à être utilisées à d'autres fins. Or, *in casu*, la finalité du traitement, contrairement à l'avis des intimés, ne ressort pas explicitement de la charte. La collecte des données est, de prime abord, en lien avec la sécurité des locaux. Le terme malversation ne peut être compris, dans ce cadre, qu'en lien avec un accès indu aux locaux, tout comme le contexte dans lequel le terme est inséré dans la charte, en lien avec un « délit » au sens du droit pénal, comme par exemple un vol, un accès indu aux locaux, une violation de domicile ou encore un dommage à la propriété. L'utilisation de « malversation », bien que signifiant un comportement humain répréhensible, ne peut donc être compris qu'en lien avec la sécurité des lieux, au vu de la formulation choisie par les EPI dans leur charte informatique et non en lien avec toute possibilité de malversation, comme avec le contrôle horaire et le respect du timbrage.

Cette conclusion est corroborée par les EPI eux-mêmes, qui indiquent qu'ils ne contrôlent pas les horaires par la porte d'entrée mais bien par l'application MOBATIME. Ils ne peuvent donc justifier sous cet angle l'usage des données à des fins de surveillance. En outre, faute de système de timbrage pour sortir du secteur, l'analyse des données est imprécise et ne peut reconstituer un horaire entier. Finalement, la recourante donne de manière convaincante plusieurs explications concernant une absence de timbrage ou une insertion manuelle des horaires, comme par exemple que l'entrée peut se faire avec plusieurs collègues, un seul ouvrant la porte pour tous, ne permettant pas de vérifier systématiquement l'entrée de chacun ni de reconstituer un horaire complet, pas plus que l'heure exacte d'arrivée. Dans ces conditions, l'utilisation de la base de données liées à la sécurité des locaux ne peut être utilisée à des fins de contrôle horaire, rendant cet usage contraire au principe de finalité. Pour ce motif déjà, le traitement est illicite.

Le préposé rappelle que les finalités du traitement doivent être reconnaissables pour la personne concernée. Cette exigence concrétise le principe de la bonne foi et augmente la transparence du traitement des données. L'art. 38 LIPAD implique que selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont être collectées. Elle doit pouvoir identifier la finalité du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances. En l'espèce, il sera tout d'abord souligné que la charte informatique des EPI ne mentionne pas la journalisation des accès au moyen de la clé électronique. En effet, le ch. 9.1 qui concerne la journalisation, indique que différentes informations sont enregistrées de manières automatiques (*sic*), à savoir « le trafic de messagerie et d'internet, les données d'authentification, les accès aux serveurs de fichiers, les statistiques d'appels téléphoniques » (ch. 9.1.1). Sous cet angle, on peut douter que la journalisation des accès liée aux clés électroniques soit ainsi conforme à la charte informatique et par conséquent licite au plan de la reconnaissabilité. En outre, il ressort du dossier que la recourante

n’a pas signé une telle quittance, ayant reçu sa clé avant l’existence de ce document. Ainsi, de ce point de vue, le principe de la bonne foi n’est pas respecté ni s’agissant de l’utilisation des données à des fins de sécurité ni à des fins de contrôle horaire. À titre superfétatoire, il sera souligné que même si la recourante avait effectivement eu connaissance du contenu de cette quittance, ce dernier ne permet pas de comprendre que les termes « en cas de soupçon de malversation » recouvrent l’utilisation des données à des fins de contrôle des horaires. On ne peut ainsi retenir, contrairement à l’avis des EPI, un lien évident, reconnaissable, entre la journalisation des données et une problématique de gestion du personnel relative aux horaires, étant rappelé que la charte informatique ne comprend pas la journalisation des entrées. Le principe de reconnaissabilité n’est ainsi pas respecté.

Finalement, le préposé peut également être suivi quand il retient que le choix d'une option de traitement moins incisif aurait dû être privilégié. Contrairement aux dires des intimés, il n’est pas exact de retenir que seul le croisement des données, au demeurant imprécis, permettait de vérifier les horaires de la recourante. Par exemple, comme mentionné par le préposé, il était loisible aux intimés de vérifier l’heure inscrite dans MOBATIME et de contrôler immédiatement l’heure réelle d’arrivée de la recourante afin de confirmer ou infirmer les soupçons du supérieur hiérarchique. Contrairement à l’avis des intimés, cet aménagement n’est ni si coûteux en temps et en argent public que cela se révèle impraticable, étant précisé que l’horaire variable de la recourante implique que ce n’est pas un timbrage horaire total inexact qui lui est reproché mais bien un timbrage d’arrivée différent de l’horaire réel d’arrivée. Le principe de la proportionnalité n’est ainsi pas respecté.

Au vu de ce qui précède, le recours sera admis, les points 2 à 4 de la décision attaquée annulés et le dossier sera renvoyé à l'autorité intimée afin qu'elle constate l’illicéité du traitement des données et procède à la destruction des données correspondantes, conformément à la recommandation du préposé.

4. Vu l'issue du litige, aucun émolument ne sera mis à la charge de la recourante qui obtient gain de cause (art. 87 al. 1 LPA). Une indemnité de procédure de CHF 1'000.- lui sera allouée, à la charge des intimés (art. 87 al. 2 LPA).

Le litige s'inscrit dans le contexte des rapports de service de la recourante. Il concerne toutefois une contestation non pécuniaire (art. 83 let. a 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 mai 2024 par A_____ contre la décision des Établissements publics pour l'intégration (EPI) du 28 mars 2024 ;

au fond :

l'admet ;

constate que l'utilisation de la journalisation des accès au moyen de la clé électronique d'A_____ à des fins de contrôle horaire constituait un traitement de données illicite ;

ordonne la destruction des fichiers récapitulant les accès d'A_____ au moyen de sa clé électronique ;

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

alloue à A_____ une indemnité de procédure de CHF 1'000.-, à la charge des EPI ;

dit que, conformément aux art. 82 ss LTF, le présent arrêt peut être porté dans les trente jours qui suivent sa notification par-devant le Tribunal fédéral :

- par la voie du recours en matière de droit public ;

- 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, av. du Tribunal-Fédéral 29, 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 Me Yann LAM, avocat de la recourante, à Me Sébastien VOEGELI, avocat des Établissements publics pour l'intégration (EPI), ainsi qu'au bureau du préposé cantonal à la protection des données et à la transparence.

Siégeant : Michèle PERNET, présidente, Florence KRAUSKOPF, Jean-Marc VERNIORY, Patrick CHENAUX, Claudio MASCOTTO, juges.

Au nom de la chambre administrative :

le greffier-juriste :	la présidente siégeant :
F. SCHEFFRE	M. PERNET

Copie conforme de cet arrêt a été communiquée aux parties.

Genève, le la greffière :