Requête en constatation du caractère illicite d'un traitement de données personnelles par le Département de l'économie et de l'emploi (DEE), alors Département du développement économique (DDE)

Recommandation du 11 mai 2021

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

1. Par mail du 14 décembre 2020, X., [redacted] du Département du développement économique (DDE), renommé Département de l'économie et de l'emploi (DEE) depuis le 30 avril 2021, a indiqué au Préposé cantonal avoir été interpellé par un journaliste à propos de ses déplacements à son bureau sis [redacted], dans le contexte de la réorganisation gouvernementale qui avait précédé. Il se disait troublé par le fait que le journaliste lui faisait savoir qu'il avait été filmé nuitamment par des caméras de vidéosurveillance lorsqu'il s'était rendu dans son bureau. Il souhaitait dès lors être renseigné sur l'éventuel usage des bandes vidéo issues du dispositif installé au [redacted] et en particulier savoir si un tel usage avait eu lieu depuis le 28 octobre 2020, en combien d'occurrences, sur l'ordre de qui, et sur quelle base légale.

2. Dans sa réponse du 15 décembre 2020, le Préposé cantonal a fait savoir au précité qu'en matière de vidéosurveillance, les compétences de l'autorité étaient limitées: l'institution concernée doit lui communiquer la liste des personnes autorisées à visionner les images (art. 42 al. 3 let. a LIPAD) et déclarer le fichier au catalogue (ce que le DDE a fait pour les deux adresses: http://outil.ge.ch/chacatfich/#/catalog/institution/214/216). Cela étant, le Préposé cantonal a expliqué que la vidéosurveillance devait répondre aux quatre conditions suivantes (art. 42 al. 1 LIPAD): a) être propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant; b) l'existence d'un système de vidéosurveillance doit être signalée de manière adéquate au public et au personnel des institutions; c) le champ de la surveillance doit être limité au périmètre nécessaire à l'accomplissement de celle-ci; d) dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques ne doivent pas rentrer dans le champ de vision des caméras ou, à défaut, doivent être rendus d'emblée non identifiables par un procédé technique approprié. Ces exigences étaient précisément répétées dans la déclaration au catalogue effectuée par le DDE. Le Préposé cantonal se proposait d'éclaircir la situation auprès de la responsable LIPAD du DDE.

3. Le même jour, le requérant a indiqué faire sienne cette proposition.

4. Dans la foulée, conformément à l'art. 23 al. 5 RIPAD, le Préposé cantonal a fait parvenir un courriel à la responsable LIPAD du DDE, dans lequel il faisait état d'une dénonciation relative à un traitement prétendument illicite de données personnelles de la part du DDE.

5. La précitée a accusé réception de ce message le même jour. Elle disait vouloir éclaircir la situation à l'interne et revenir à l'autorité dans les meilleurs délais.

6. Le 22 décembre 2020, le demandeur a écrit au Préposé cantonal avoir « *obtenu de façon informelle et unilatérale l'information qu'au moins une extraction d'images me concernant aurait été ordonnée pour le 25 ou le 26 novembre dernier* ».

7. A la même date, Y., [redacted] du Département des finances et des ressources humaines (DF) ainsi que du DDE depuis la réorganisation intervenue au sein du Gouvernement, a fait savoir au Préposé cantonal qu'elle allait se déterminer la semaine du 11 janvier 2021.

8. Relancé le 23 décembre 2020 par le demandeur, le Préposé cantonal lui a indiqué ce qui précède.

9. Le 12 janvier 2021, Y. a fait savoir en substance ce qui suit au Préposé cantonal: la dénonciation semblait mue par des fins étrangères au but de la LIPAD, de sorte qu'aucune suite ne devrait y être donnée. Elle a ajouté toutefois que le visionnage des images était licite au vu des circonstances préoccupantes qui l'ont justifié, à savoir que le dénonciateur s'était rendu nuitamment, à une reprise dans son ancien bureau, ce qui était étrange considérant que « *1) à la suite des mesures organisationnelles prises par le Conseil d'Etat lors de sa séance du 28 octobre 2020, il n'était plus supposé avoir accès à son bureau et qu'interdiction lui avait été signifiée d'entrer en contact avec ses anciens collaborateurs et collaboratrices, que 2) possibilité lui avait d'ores et déjà été donnée de récupérer ses affaires personnelles et autres documents privés s'y trouvant et que 3) un bureau avait été mis immédiatement à sa disposition dans un autre bâtiment* ». Dès lors, il importait de visionner les images afin de comprendre les circonstances de cette « *intrusion nocturne* ». Elle précisait que les images avaient été visionnées à une seule reprise par elle-même et avaient montré que le dénonciateur « *s'était introduit dans ses anciens locaux muni d'une sacoche et en était ressorti – plus d'une heure plus tard – avec deux sacs pleins* ». Ce visionnage était licite, en sa qualité de [redacted] du DDE et du DF (art. 42 al. 4 let. a LIPAD).

10. Le 13 janvier 2021, le Préposé cantonal a indiqué à la susnommée qu'au vu de l'art. 44 al. 1 LIPAD, il convenait de communiquer à la personne concernée qu'elle figurait sur des images de vidéosurveillance de la nuit du 26 novembre 2020 et que lesdites images avaient été visionnées. Par ailleurs, il s'agissait également de lui préciser la base légale sur laquelle ce visionnement était intervenu. Le Préposé cantonal se proposait de transmettre directement ces éléments au dénonciateur.

11. Par courriel du 14 janvier 2021, Y. disait effectivement préférer que l'autorité communique directement les informations au dénonciateur.

12. Le 15 janvier 2021, le Préposé cantonal a rédigé un mail à l'attention du demandeur, dans lequel il était notamment écrit: « *Le DDE a communiqué à notre autorité les éléments suivants - Vous figurez sur les images de vidéosurveillance du système installé dans les locaux de l'immeuble de la* [redacted] *la nuit du jeudi 26 novembre 2020. - Ces images ont été visionnées à une reprise par Y., conformément aux art. 42 al. 3 LIPAD et 42 al. 4 let. a LIPAD. Si vous entendez faire valoir des prétentions selon les art. 44 ss LIPAD, il convient, comme le prévoit la loi, de vous adresser dans un premier temps à la précitée. Copie du présent message sera adressée à cette dernière* ».

13. Le 22 janvier 2021, le précité a fait savoir au Préposé cantonal qu'il ressortait des écrits du DDE que ce dernier n'invoquait pas le constat d'une atteinte aux biens ou aux personnes pour justifier le visionnage des images, d'une part, et avouait que les images ont été visionnées par une personne qui ne figure pas sur la liste des personnes dûment autorisées et communiquée au Préposé cantonal, d'autre part. Il ajoutait que « *Se pose*

à mon sens la question de savoir si ce traitement de données est également contraire à l'art. 42 al. 3 et 4 LIPAD. Le fait que les images aient été visionnées en l'absence de toute atteinte n'est pas, en soi, contraire à l'art. 42 LIPAD. J'y vois, par contre, une violation du principe de la proportionnalité, car un tel visionnement n'était justifié par aucun intérêt public (…) J'y vois également, bien évidemment, une violation du principe de la transparence ou de la bonne foi (venire contra factum proprium), car le DDE n'a pas respecté sa propre déclaration. Il y a donc, à tout le moins et à ce stade de mon analyse, une violation des principes généraux de traitement qui ne saurait être légitimée par aucun motif justificatif. Le fait que les images aient été visionnées par une personne non autorisée constitue, en soi, une violation de l'art. 42 al. 3 let. a LIPAD, car, soit [redacted] *ne figurait pas sur la liste (seuls les membres de la police y figurent), soit la liste a été modifiée pour l'y inclure, mais n'a pas été communiquée au Préposé. Dans les deux hypothèses, l'art. 42 al. 3 LIPAD est violé. Le DDE invoque singulièrement l'art. 42 al. 4 LIPAD ("La communication des données peut avoir lieu en dérogation des règles générales de communication des données s'il s'agit de renseigner notamment les instances hiérarchiques supérieures dont l'institution dépend") pour justifier le visionnement de ces images par* [redacted]*. Il faut bien reconnaître qu'il s'est agi, en l'occurrence, de renseigner* [redacted]*, qui est également* [redacted] *du DDE. A mon avis, toutefois, le visionnement des images ne constitue pas la même opération de traitement que la communication des données. La communication des données prévue à l'art. 42 al. 4 LIPAD ne concerne pas le premier visionnement des images, qui doit permettre d'élucider une infraction à l'origine d'une atteinte aux personnes et/ou aux biens détectée par un autre moyen que la vidéosurveillance (p. ex. constat visuel, technique ou médical; quand une vitre est brisée, on n'a pas besoin de la vidéosurveillance pour le remarquer). La communication, ultérieure, des images obtenues à l'instance hiérarchique supérieure vise un but d'information, lorsque l'existence de faits susceptibles de constituer une infraction est confirmée par le premier visionnement. Cette information peut permettre, soit de porter l'affaire à un niveau hiérarchique suffisant pour disposer de la compétence de déposer plainte ou non, soit de prendre des sanctions administratives (avertissement, suspension, licenciement, etc.) à l'égard d'un auteur d'atteintes aux biens ou aux personnes qui serait également employé de l'Etat de Genève. Le visionnement par* [redacted] *ne saurait dès lors être justifié, en tant que communication de données licite, en vertu de l'art. 42 al. 4 LIPAD. J'en conclus que nous sommes en présence d'un traitement de données illicite* ».

14. Le 25 janvier 2021, le Préposé cantonal a indiqué au demandeur qu'il lui fallait s'adresser, dans un premier temps, au DDE, comme le commandait l'art. 49 LIPAD, reproduit, car il n'avait pas la compétence, à ce stade, d'établir formellement si un traitement illicite avait été commis. Il ajoutait que ce n'est que s'il n'était pas intégralement fait droit à ses prétentions que l'autorité pouvait être saisie. Il terminait en se disant prêt à organiser une rencontre avec la responsable LIPAD du DDE (ou [redacted]), si cela était considéré comme opportun.

15. Le 1er février 2021, le dénonciateur a sollicité de la responsable LIPAD du DDE qu'elle lui transmette, sans délai et intégralement, tous les éléments relatifs à ses données personnelles afférentes à la situation, « *soit les conditions, circonstances et déclenchement de leur accès, le constat du caractère illicite de leur traitement ainsi que ses tenants et aboutissants, la fin de ce traitement illicite ainsi que la suppression de ses effets. Je voudrais également connaître ce qu'il est advenu de leur éventuelle destruction, en date et en heure. Enfin, je souhaite savoir s'il a été porté plainte pour violation du secret de fonction, vu la résonance médiatique de cette situation* ».

16. Le 12 février 2021, Y. a en substance repris l'argumentation de son courriel du 12 janvier 2021 adressé au Préposé cantonal. Elle a ajouté que les images n'étaient à ce

jour plus disponibles, car conservées uniquement sept jours, puis écrasées par les suivantes et que « *En ma qualité de* [redacted] *du DDE et du DF, j'étais habilitée à recevoir la communication desdites bandes et à les visionner (art. 42 al. 4 let. a LIPAD). Seul un cercle (très limité) de personnes a eu accès à ces bandes de vidéosurveillance, à une reprise si bien que ce visionnage respecte le principe de la proportionnalité; il répondait en outre à un intérêt public évident compte tenu des circonstances. L'Office cantonal des Bâtiments (OCBA) nous a par ailleurs indiqué qu'une liste des « personnes habilitées » à visionner les images du système de vidéosurveillance en question avait été communiquée au Préposé cantonal à la protection des données et à la transparence, lors de la mise en place dudit système de surveillance. Il s'agissait en particulier du Directeur au sein de la Direction de l'organisation et de la sécurité de l'information, de la logistique et de la gestion des risques et de la qualité (DOSIL) et du responsable logistique au sein de la DOSIL, toutes personnes étant hiérarchiquement subordonnées au Conseil d'Etat. Il semblerait que, à la suite des changements intervenus dans la répartition des départements à compter de janvier 2019, la liste des personnes autorisées n'ait pas encore été mise à jour. En conclusion, tant le visionnage que le traitement des bandes de vidéosurveillance installées dans le bâtiment de* [redacted] *échappent à toute critique; ils étaient parfaitement licites. (…) Pour le surplus, il n'y a eu aucune dénonciation auprès de l'autorité pénale en rapport avec cette affaire* ».

17. Le 6 mars 2021, le demandeur a réitéré qu'aucune atteinte aux personnes et/ou aux biens n'a été constatée dans les locaux sis à [redacted] entre le 26 novembre et le 1er décembre 2020 et, qu'en conséquence, les images avaient été visionnées de manière illicite. Il a ajouté qu'aucune décision d'interdiction d'accès aux locaux ne lui a été notifiée, soulignant qu'il disposait encore des moyens d'entrer de manière licite dans les locaux à ce moment-là. Il s'est interrogé sur la source de l'information selon laquelle il était présent dans les locaux ce soir-là, cette dernière n'ayant pas été divulguée et en conclut qu'une autre personne a forcément dû visionner les images et qu'il s'agit alors de la « *pratique d'une surveillance illicite généralisée, et, par conséquent, disproportionnée, des entrées et sorties du bâtiment susmentionné* ». Il écrit enfin, s'agissant de l'art. 42 al. 4 LIPAD que *« si le premier visionnement des images litigieuses est déjà illicite (car disproportionné) en l'occurrence en raison de l'absence d'atteinte aux personnes ou aux biens, toute communication ultérieure de ces images est également illicite ».* En conséquence, il conclut par sa volonté de saisir le Préposé cantonal pour constatation de ce comportement illicite et solliciter une recommandation.

18. Le 8 mars 2021, le Préposé cantonal a indiqué au requérant que si la LIPAD n'imposait une médiation qu'en matière de transparence, s'agissant de contentieux concernant la protection des données personnelles, selon l'exposé des motifs de la loi, « *Le fait de demander au responsable de saisir le Préposé cantonal n'exclut pas un dialogue entre les différentes parties concernées ni un certain bon sens, pas plus que des échanges réguliers et informels avec ce dernier, ce qui, à terme, permettra aussi d'harmoniser le plus possible les solutions retenues* » (MGC 2005-2006 X A 8520). Le Préposé cantonal désirait de la sorte inviter le susnommé à une rencontre de médiation, option qu'il avait préalablement soumise à Y., laquelle s'était dite ouverte à un tel processus.

19. Le 10 mars 2021, X. a fait savoir qu'il acceptait volontiers cette proposition de médiation.

20. La rencontre de médiation a eu lieu le 22 avril 2021 en présence de X., Y., de la Préposée adjointe et du Préposé cantonal.

21. Elle n'a pas abouti, le requérant souhaitant la rédaction d'une recommandation.

22. Le 26 avril 2021, ce dernier a fait parvenir au Préposé cantonal deux brefs échanges de courriels datant de décembre 2020. Etait notamment fait état d'un changement de serrures dans son bureau postérieur au 26 novembre 2020.

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

23. 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 à 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.

24. En 2008, la loi a fait l'objet d'une révision importante, entrée en vigueur le 1er janvier 2010: 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.

25. La LIPAD est applicable aux institutions publiques genevoises, en particulier aux *« pouvoirs exécutif, législatif et judiciaire cantonaux, ainsi que leurs administrations et les commissions qui en dépendent* » (art. 3 al. 1 let. a LIPAD).

26. A teneur de l'art. 1 al. 1 let. f du règlement sur l'organisation de l'administration cantonale du 1er juin 2018 (ROAC; RSGe B 4 05.10), le Département de l'économie et de l'emploi (Département du développement économique, DDE, au moment des faits) fait partie de l'administration cantonale, de sorte qu'il est soumis à la LIPAD.

27. 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 let. 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.

28. Ainsi, les images d'une personne identifiable sur des enregistrements de vidéosurveillance sont des données personnelles au sens de l'art. 4 let. a LIPAD.

29. La loi énonce un certain nombre de principes généraux régissant la protection des données personnelles (art. 35 à 40 LIPAD), soit en particulier:

- **Légalité** (art. 35 al. 1 LIPAD). Les institutions publiques ne peuvent traiter de telles données que si l'accomplissement de leurs tâches légales le rend nécessaire.
- **Bonne foi** (art. 38 LIPAD). Les données doivent avoir été obtenues de manière loyale, en toute connaissance des personnes concernées.
- **Proportionnalité** (art. 36 LIPAD). Seules peuvent être collectées les données personnelles aptes et nécessaires à atteindre un but déterminé.
- **Finalité** (art. 35 al. 1 LIPAD). Les données personnelles ne doivent être traitées que dans le but indiqué lors de leur collecte, prévu par une loi ou qui ressort des circonstances.
- **Exactitude** (art. 36 LIPAD). Quiconque traite des données personnelles doit s'assurer qu'elles sont correctes (par exemple qu'elles ont été saisies correctement ou qu'il n'y a pas eu confusion). A défaut, elles doivent être corrigées ou mises à jour.

- **Sécurité** (art. 37 LIPAD). Les données doivent être protégées, tant sur le plan technique que juridique, conformément aux risques présentés par la nature des données en cause, à la lumière de l'ingérence à la sphère privée des personnes concernées.
- **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. Ce dernier principe touche précisément le droit à l'oubli, selon lequel, dans un cas particulier, certaines informations n'ont plus à faire l'objet d'un traitement par l'institution publique concernée

30. La vidéosurveillance touche immanquablement certains droits fondamentaux, particulièrement le droit au respect de la sphère privée et la liberté personnelle (art. 10 al. 2 et 13 Cst.), lesquels protègent notamment l'intégrité physique et psychique d'un individu, sa liberté de mouvement, toutes les informations le concernant qui ne sont pas accessibles au public, les données d'identification et la correspondance privée. Le recours à la vidéosurveillance doit précisément respecter ces libertés de manière générale.

31. L'installation d'un dispositif de vidéosurveillance nécessite une base légale précise, afin de respecter les dispositions précitées (voir à ce propos Cour eur. D.H., Perry, du 17 juillet 2003). Suite à l'arrêt rendu par le Tribunal fédéral en la cause 1C.315/2009 du 13 octobre 2010, si une base légale matérielle (règlement ou directive) suffit pour l'installation d'un dispositif de vidéosurveillance qui ne permet pas l'enregistrement des images, une base légale formelle est nécessaire pour l'installation d'un dispositif qui le permet.

32. La Cour européenne des droits de l'homme a rendu plusieurs arrêts relatifs à la vidéosurveillance. Pour elle, le fait de surveiller les actes d'un individu dans un lieu public en utilisant un système de prise de vues sans enregistrer de données visuelles n'entraîne pas en soi une ingérence dans la vie privée de l'individu (Cour eur. D.H., Peck, du 28 janvier 2003, § 59). En revanche, la vidéosurveillance effectuée par l'employeur à l'insu d'une salariée, pendant environ cinquante heures sur une période de deux semaines et l'utilisation de l'enregistrement obtenu dans la procédure devant les juridictions du travail pour justifier son licenciement, constituent une atteinte au droit de l'intéressée au respect de sa vie privée (Cour eur. D.H., Köpke, du 5 octobre 2010). Il en va pareillement de la vidéosurveillance non dissimulée de professeurs d'université pendant qu'ils dispensaient leurs cours, dont les enregistrements étaient conservés pendant un mois et consultables par le doyen de la faculté (Cour eur. D.H., Antović et Mirković, du 28 novembre 2017, § 44 s.). L'instance alsacienne a aussi défini, à l'attention des juridictions nationales, des facteurs à prendre en compte pour s'assurer de la proportionnalité de mesures de vidéosurveillance sur le lieu de travail (Cour eur. D.H., López Ribalda et autres, du 17 octobre 2019, § 116).

33. En 2016, le Tribunal fédéral avait jugé, s'agissant de caméras de vidéosurveillance installées dans un immeuble locatif, qu'en présence d'un nombre restreint de locataires et fautes d'indices suggérant l'existence d'un risque concret de cambriolages ou d'actes de vandalisme, l'atteinte à la sphère privée liée à la vidéosurveillance dans la zone d'entrée et les passages intérieurs était excessive; l'intérêt des bailleurs et des locataires qui ont consenti à la mesure était suffisamment préservé grâce aux neuf caméras restantes, dont deux étaient situées dans la cour extérieure donnant sur les trois entrées d'immeuble (ATF 142 III 263, cons. 2.2.1 et 2.2.2).

34. La LIPAD comprend une disposition spécifique relative à la vidéosurveillance, mettant en œuvre les principes susmentionnés dans le cadre de l'utilisation de cette technologie.

Aux termes de l'art. 42 LIPAD, « *[1] Dans la mesure où elles ne sont pas dictées par l'accomplissement légal de tâches au sens de l'article 35, la création et l'exploitation d'un système de vidéosurveillance ne sont licites que si, cumulativement: a) la vidéosurveillance est propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant; b) l'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions; c) le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci; d) dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié. [2] L'éventuel enregistrement de données résultant de la surveillance doit être détruit en principe dans un délai de 7 jours. Ce délai peut être porté à 3 mois en cas d'atteinte avérée aux personnes ou aux biens et, en cas d'ouverture d'une information pénale, jusqu'à l'issue de la procédure. [3] Les responsables des institutions prennent les mesures organisationnelles et techniques appropriées afin de: a) limiter le visionnement des données, enregistrées ou non, à un cercle restreint de personnes dûment autorisées, dont la liste doit être régulièrement tenue à jour et communiquée au préposé cantonal; b) garantir la sécurité des installations de surveillance et des données éventuellement enregistrées. [4] En dérogation à l'article 39, la communication à des tiers de données obtenues au moyen d'un système de vidéosurveillance ne peut avoir lieu que s'il s'agit de renseigner: a) les instances hiérarchiques supérieures dont l'institution dépend; b) les autorités judiciaires, soit aux conditions de l'article 39, alinéa 3, soit aux fins de dénoncer une infraction pénale dont la vidéosurveillance aurait révélé la commission* ».

35. Le droit d'accès aux données personnelles institué par l'art. 44 LIPAD traite de la possibilité pour une personne de demander au responsable de l'institution publique requise si des données la concernant sont traitées et, le cas échéant, que soient communiquées: « *a) toutes les données la concernant contenues dans un fichier, y compris les informations disponibles sur l'origine des données; b) sur demande, les informations relatives au fichier considéré contenues dans le catalogue des fichiers* » (art. 44 al. 2 LIPAD).

36. A la forme, l'art. 45 LIPAD prévoit que « *la communication de ces données et informations doit être faite sous une forme intelligible et, en règle générale, par écrit et gratuitement* ».

37. L'art. 47 LIPAD détermine, par ailleurs, 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.

38. Selon l'art. 49 al. 1 LIPAD, toute requête fondée sur l'art. 44 doit être adressée par écrit au responsable en charge de la surveillance de l'organe dont relève le traitement considéré. Conformément à l'al. 2, le responsable saisi traite la requête avec célérité. S'il y a lieu, il la transmet au responsable compétent. A teneur de l'al. 3, s'il fait intégralement droit aux prétentions du requérant, il l'en informe. Par contre, selon l'al. 4, s'il n'entend pas y faire intégralement droit ou en cas de doute sur le bien-fondé de

celles-ci, il transmet la requête au Préposé cantonal avec ses observations et les pièces utiles. Enfin, l'art. 49 al. 5 LIPAD précise que « *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* ».

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

39. Conformément à l'art. 47 al. 1 let. c LIPAD, le requérant entend exiger du Département de l'économie et de l'emploi qu'il constate le caractère illicite du traitement de données le concernant. Il considère en effet que des images de lui issues d'un dispositif de vidéosurveillance ont été visionnées sans qu'une atteinte aux biens ou aux personnes n'ait été préalablement constatée et que, partant, un tel visionnement était illicite.

40. Les Préposés relèvent, à propos de la constatation du caractère illicite de l'atteinte, que ce moyen est celui de l'art. 28a al. 1 let. c CC (voir aussi le renvoi général de l'art. 15 al. 1 LPD *ab initio*).

41. Cette action est recevable dès que la personne concernée a un intérêt digne de protection à mettre fin à un trouble latent à la personnalité, indépendamment de la gravité du trouble (ATF 127 III 481 (486), JdT 2002 I 426 (429); TF, 5A_605/2007 du 4 décembre 2008, consid. 3.2; Philippe Meier, Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N. 1753). La jurisprudence définit le « trouble latent » comme suit: « *Ce qui importe, c'est que le trouble ne disparaisse pas de lui-même avec l'écoulement du temps et continue, par exemple, à avoir un effet dévalorisant pour la personne (ATF 95 II 481 c. 9, p. 497, rés. JdT 1971 I 226, p. 232; ATF 123 III 354 c. 1e, p. 360, non rés. sur ce point au JdT 1998 I 333). Le risque est accru, de nos jours, en ce qui concerne les médias, vu qu'un accès général aux archives est possible grâce aux moyens techniques (ATF 123 III 354 c. 1f, p. 361, rés. JdT 1998 I 333, c. 1d, p. 336). (…). Seul supprimerait, au demeurant, l'intérêt à l'action, le fait que les circonstances auraient tellement changé que l'information causant une atteinte aurait perdu toute signification. Cela permettrait alors d'exclure toute nouvelle publication (ATF 123 III 354 c. 1g, p. 362, rés. JdT 1998 I 333 c. 1d, p. 336)* » (ATF 127 III 481 (486), JdT 2002 I 426 (429). La persistance du trouble est donnée notamment lorsque « *des tiers peuvent avoir connu l'atteinte (par ex. la diffusion d'une photo ou d'un livre) et en retirer de façon durable une impression défavorable concernant tel ou tel aspect de la personnalité de la victime: le mal est fait et n'est plus à faire, mais ses conséquences perdurent. La victime trouvera alors protection dans le constat judiciaire de ce que l'atteinte était illicite* » (CR CC I-Jeandin, art. 28a, n°11).

42. L'existence d'une faute ou le respect d'un délai ne sont pas pertinents (Laurent Rieben, La protection de la personnalité contre les atteintes par voie de presse au regard des dispositions du code civil et de la loi contre la concurrence déloyale, SJ 2007 II, p. 225).

43. En l'occurrence, les images du requérant issues des caméras de vidéosurveillance installées au [redacted] et datées du 26 novembre 2020 constituent des données personnelles au sens de l'art. 4 let. a LIPAD. Elles ne sont plus disponibles, car elles n'ont pas été conservées au-delà de sept jours. Toutefois, l'existence et le visionnement desdites images ont fait l'objet de mentions dans la presse.

44. Au vu de ce qui précède, il n'est pas contestable que le demandeur possède un intérêt digne de protection à ce qu'il soit constaté si un trouble a été subi.

45. Il convient toutefois d'examiner si ce trouble constitue un traitement au caractère illicite au sens de l'art. 47 al. 1 let. c LIPAD.

46. Comme susmentionné au point 34, à Genève, l'art. 42 LIPAD constitue la base légale formelle idoine en matière de vidéosurveillance. Selon son al. 1, la vidéosurveillance doit répondre aux quatre conditions suivantes (art. 42 al. 1 LIPAD): a) elle est propre et nécessaire à garantir la sécurité des personnes et des biens se trouvant dans ou à proximité immédiate de lieux publics ou affectés à l'activité d'institutions publiques, en prévenant la commission d'agressions ou de déprédations et en contribuant à l'établissement des infractions commises le cas échéant; b) l'existence d'un système de vidéosurveillance est signalée de manière adéquate au public et au personnel des institutions; c) le champ de la surveillance est limité au périmètre nécessaire à l'accomplissement de celle-ci; d) dans l'accomplissement de leurs activités à leur poste de travail, les membres du personnel des institutions publiques n'entrent pas dans le champ de vision des caméras ou, à défaut, sont rendus d'emblée non identifiables par un procédé technique approprié. En outre, l'éventuel enregistrement de données résultant de la surveillance doit être détruit en principe dans un délai de sept jours (art. 42 al. 2 LIPAD).

47. Les Préposés observent qu'en 2016, le Département du développement économique a déclaré au catalogue des fichiers tenus par le Préposé cantonal selon l'art. 43 LIPAD un fichier intitulé « *vidéosurveillance* », destiné à « *permettre d'assurer et garantir la sécurité dans le bâtiment de la* [redacted] ». Ce système, dont la mise en œuvre effective est intervenue en septembre 2016, comprend quinze caméras dans les cages d'escaliers et couloirs, filmant 7 jours/7 et 24 heures/24. L'entrée dans la zone sous vidéosurveillance est signalée au moyen d'affichettes. Il est précisé que les images, qui ne sont pas visionnées en direct ni de manière différée, sont conservées pendant sept jours et sont écrasées par les suivantes. Il est encore indiqué que, dans l'éventualité d'une atteinte aux biens ou aux personnes, il est fait appel à la police, laquelle est seule habilitée à visionner les images servant à élucider l'infraction commise.

48. Les Préposés constatent en conséquence que les exigences de l'art. 42 al. 1 et 2 LIPAD ont précisément été répétées dans la déclaration au catalogue effectuée par le DDE et que l'installation apparaît conforme aux exigences légales sur ces points. Par ailleurs, ce n'est pas la licéité de l'existence du système de vidéosurveillance dans les locaux qui est remise en question par le demandeur, mais bien la licéité du visionnement d'images de la nuit du 26 novembre 2020, images sur lesquelles il figurait. Cette dernière question doit être examinée à l'aune de la finalité de l'installation de vidéosurveillance et des circonstances particulières du cas d'espèce.

49. L'art. 42 LIPAD ne prévoit pas expressément les situations justifiant que les images soient visionnées; il mentionne uniquement la limitation du visionnement à un cercle restreint de personnes dûment autorisées (al. 3 let. a), point traité ci-dessous. Toutefois, il convient de retenir qu'un visionnement ne saurait intervenir que dans le but pour lequel le système de vidéosurveillance a été installé, faute de quoi les exigences de l'art. 42 al. 1 se trouveraient dénuées de tout fondement.

50. Tout d'abord, comme le démontrent les échanges de courriels remis aux Préposés, il sied de remarquer que, dans sa séance du 28 octobre 2020, le Conseil d'Etat a pris des mesures organisationnelles retirant à X. [redacted] DDE pour la confier à Y. Possibilité lui avait été donnée de récupérer ses affaires personnelles et autres documents privés se trouvant dans son bureau. Enfin, un local lui avait été immédiatement mis à disposition dans un autre bâtiment, car X. n'était plus censé avoir accès à son bureau dans le bâtiment sis [redacted].

51. Y. explique, dans ses courriels des 12 janvier et 12 février 2021, avoir été informée le 1er décembre 2020 que X. s'était rendu, au moins la nuit du 26 novembre 2020, dans son

ancien bureau. Dès lors que ce dernier n'était plus supposé avoir accès à son bureau, tout du moins sans son autorisation ou une information à ce propos, la susnommée a exigé de pouvoir visionner, à une reprise uniquement, les bandes de vidéosurveillance de la nuit en question. Il en est ressorti que, selon elle, X. s'était introduit dans ses anciens locaux muni d'une sacoche et en était ressorti avec deux sacs pleins, alors même qu'il avait déjà pu emporter avec lui ses affaires et ses documents personnels lorsque la responsabilité du DDE lui avait été retirée. Ultérieurement, des mesures ont été prises pour empêcher l'accès du demandeur à son bureau.

52. Au vu des documents en leur possession et des explications fournies, les Préposés comprennent que Y. a considéré que le précité se rendait dans son bureau alors qu'il n'était plus supposé s'y rendre, pour y travailler et emmener des documents professionnels, ce qui l'a amenée à visionner les images querellées et confirmer les soupçons. Ils comprennent donc que c'est suite à des indices suggérant l'existence d'un risque que le susnommé emporte avec lui des dossiers relatifs à son ancienne charge que le visionnage est intervenu. L'on peut de la sorte considérer que le visionnement des images a été effectué, selon les explications fournies par Y., dans le but de garantir la sécurité des biens de l'Etat. Dès lors, opéré dans un tel but, le traitement ne présente pas de caractère illicite, même s'il s'agit d'un cas qu'il sied de qualifier de limite, dans la mesure où la proportionnalité d'un tel visionnement peut être questionnée. Toutefois, à cet égard, les Préposés relèvent que les images n'ont été visionnées qu'à une seule reprise et ont été détruites, conformément aux exigences de l'art. 42 al. 2 LIPAD. De plus, le système de vidéosurveillance lui-même a été installé conformément à l'art. 42 al. 1 LIPAD. Ils sont donc d'avis que l'atteinte à la sphère privée liée au visionnement des images de vidéosurveillance ne peut être en l'espèce considérée comme illicite ou disproportionnée.

53. S'agissant du cercle restreint de personnes pouvant avoir accès aux images (art. 42 al. 3 let. a LIPAD), les Préposés notent que le catalogue des fichiers indique uniquement la police. Dans son message du 12 janvier 2021, Y. relève que l'Office cantonal des Bâtiments (OCBA) a fait parvenir aux Préposés, en 2016, une liste des personnes habilitées à visionner les images du système de vidéosurveillance en question, comprenant le Directeur au sein de la Direction de l'organisation et de la sécurité de l'information, de la logistique et de la gestion des risques et de la qualité (DOSIL) et le responsable logistique au sein de la DOSIL. Cette liste n'était toutefois pas à jour. Quoi qu'il en soit, les Préposés observent que la précitée ne fait pas partie des personnes pouvant avoir accès aux images.

54. Cela étant, les Préposés sont d'avis qu'en sa qualité de [redacted] DDE et de supérieure hiérarchique du Directeur et du responsable logistique de la DOSIL, Y. était habilitée à recevoir la communication desdites bandes et à les visionner selon l'art. 42 al. 4 let. a LIPAD.

55. Dès lors, au vu de ce qui précède, le Préposé cantonal recommande au Département de l'économie et de l'emploi de ne pas donner une suite favorable à la requête en constatation du caractère illicite du traitement des images de vidéosurveillance.

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande au Département de l'économie et de l'emploi de ne pas donner suite à la requête en constatation du le caractère illicite du traitement des images de vidéosurveillance.

Dans les 10 jours à compter de la réception de la présente recommandation, le Département de l'économie et de l'emploi doit rendre une décision sur les prétentions du requérant.

La présente recommandation est notifiée par pli recommandé à:

- Y., Département des finances et des ressources humaines (DF), Secrétariat général, Place de la Taconnerie 7, Case postale 3860, 1211 Genève 3
- X., [redacted]

Stéphane Werly
Préposé cantonal

Joséphine Boillat
Préposée adjointe

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