Bulletin d'information, n° 42, juin 2016

Le Préposé cantonal à la protection des données et à la transparence (PPDT) vous adresse son bulletin d'information. Celui-ci est destiné aux personnes intéressées des institutions publiques cantonales et communales du canton de Genève.

Diffusé quatre fois par an, ce bulletin d'information renseigne sur les actualités relatives aux deux domaines d'action du PPDT, soit la transparence, d'une part, et la protection des données personnelles, d'autre part.

Une clause contractuelle de confidentialité ne permet pas d'échapper à la transparence : la Chambre administrative admet le recours d'un particulier souhaitant obtenir le coût des abonnements à des revues scientifiques payé par l'Université de Genève - arrêt du 23 février 2016 - ATA/154/2016

G. souhaitait obtenir de l'Université de Genève les documents propres à le renseigner sur les prix qu'elle a payés entre 2010 et 2016 aux éditeurs Elsevier B.V., Springer Science+Business Media et Wiley-VCH Verlag GmbH Co. KGaA pour bénéficier des abonnements à leurs revues.

Le 20 novembre 2014, la Préposée adjointe avait recommandé à l'UNIGE de faire droit à cette demande. Elle rappelait que la transparence est particulièrement importante pour tout ce qui relève de la gestion financière des institutions, ce domaine intéressant particulièrement la libre formation de l'opinion des citoyens sur la bonne gestion des institutions,

L'UNIGE avait décidé de ne pas suivre la recommandation. Selon elle, des intérêts prépondérants de tiers s'opposaient à l'accès aux documents sollicités. En particulier, consentir un tel accès serait propre à révéler des informations couvertes par des secrets professionnels, de fabrication ou d'affaires, le secret fiscal, le secret bancaire ou le secret statistique au sens de l'art. 26 al. 2 litt. i LIPAD.

Sa décision a fait l'objet d'un recours auprès de la Chambre administrative.

Dans son arrêt, cette dernière relève que l'UNIGE ne saurait se prévaloir des clauses de confidentialité figurant dans les contrats conclus par le Consortium des bibliothèques universitaires suisses en son nom avec les éditeurs susmentionnés. En effet, ces clauses de confidentialité ne sont pas absolues et réservent l'application de dispositions légales imposant la communication de leur contenu, comme en matière de législation sur la transparence.

Par ailleurs, de telles clauses ne sauraient faire échec au principe de transparence, sous peine de le vider de sa substance et de permettre aux parties à un contrat de choisir les informations qu'elles souhaitent divulguer, alors même que la LIPAD a pour but de renverser le principe du secret de l'administration pour faire primer celui de la transparence.

Pour les juges, "*un tel mode de faire constituerait une fraude à la loi*".

De surcroît, l'UNIGE ne démontre en rien la matérialité ni la possible réalisation d'un préjudice en cas de divulgation figurant dans les contrats. Qui plus est, les maisons d'édition susmentionnées se sont désintéressées de la procédure, étant donné l'absence de réaction de deux d'entre elles suite à leur appel en cause et à la position à la limite du formaliste excessif de la troisième.

La Chambre administrative ordonne donc à l'Université de donner accès à G. à tout document susceptible de le renseigner sur les prix qu'elle a payés entre 2010 et 2016 aux trois éditeurs pour bénéficier des abonnements à leurs revues.

http://justice.geneve.ch/tdb/Decis/TA/FichierWord/2016/0001/ATA_000154_2016_A_170_2015.pdf

~~~
~~~

Recommandations du Préposé cantonal en matière de transparence

Selon l'art. 10 al. 2 RIPAD, les recommandations du Préposé cantonal ainsi que les décisions liées à la requête peuvent être rendues publiques une fois prise la décision de l'institution publique concernée.

- Recommandation du 25 février 2016 relative à une ***demande d'accès à des documents de la Commission de surveillance des professions de la santé et des droits des patients (CSPSDP) :***

  Les faits relatifs à la présente affaire étaient relativement complexes. Le requérant, un psychiatre radié du registre des médecins autorisés à exercer à Genève à la suite d'une plainte pénale d'un patient, souhaitait obtenir un accès complet à son dossier comprenant des documents datant d'il y a près de dix ans relatifs à la procédure de levée du secret médical de ses patients (notamment les courriers échangés entre eux et la CSPSDP). Après examen des pièces du dossier auxquelles la Commission n'avait pas donné accès au demandeur, la Préposée adjointe a pu confirmer qu'aucun échange ne concernait le droit d'accès aux données personnelles propres du requérant. Elle a estimé que c'était à juste titre que les échanges entre les patients du psychiatre et l'autorité ne lui avaient pas été remis, car ceux-ci relèvent strictement de la sphère privée de chacune de ces personnes. Elle est ainsi arrivée à la conclusion, quel que soit l'angle sous lequel la requête du demandeur était examinée, qu'il n'était pas possible d'y répondre favorablement parce que l'intérêt au respect de la sphère privée des patients s'opposait à la communication des documents demandés.
  https://www.ge.ch/ppdt/doc/documentation/Recommandation-25-fevrier-2016.pdf

- Recommandation du 11 avril 2016 relative à une ***demande d'accès à des documents internes Police :***

  Interpellé par quatre gendarmes en 2014, le demandeur souhait obtenir le rapport sur l'intervention rédigé par l'Etat-major de la Gendarmerie et adressé à Mme la Cheffe de la Police, document qui a servi de base à cette dernière pour conclure que les fonctionnaires avaient accompli leur mission dans le respect des normes légales et des dispositions réglementaires applicables à ce type d'événement. In casu, le Préposé cantonal s'est étonné de la démarche suivie par le conseil du requérant, laquelle n'avait pas de rapport avec le but poursuivi par l'art. 1 al. 2 litt. a LIPAD, à savoir favoriser la libre formation de l'opinion publique et la participation des citoyens à la vie publique. Présentement, la requête avait trait au second objectif poursuivi par la LIPAD, à savoir protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant. Le Préposé cantonal a suivi le raisonnement de Mme la Cheffe de la police: si tout un chacun a la possibilité de consulter son dossier de police, lequel contient tous les événements l'impliquant, un rapport de synthèse et les notes internes relatifs à un événement ne peuvent pas être considérés comme des dossiers de police au sens de la loi sur les renseignements et les dossiers de police et la délivrance des certificats de bonne vie et mœurs du 29 septembre 1977 (LCBVM; RSGE F 1 25) prise comme une lex specialis; ils échappent à son champ d'application. Le Préposé cantonal a donc recommandé à la Police cantonale de maintenir son refus de communiquer les documents considérés.
  http://www.ge.ch/ppdt/doc/documentation/Recommandation-11-avril-2016.pdf

Recommandations du Préposé cantonal en matière de protection des données personnelles

Selon l'art. 20 RIPAD, les recommandations du Préposé cantonal ne peuvent faire l'objet d'une publication tant et aussi longtemps que l'affaire est susceptible de recours et, en cas de recours, qu'elles ne sont pas définitivement tranchées par les autorités judiciaires. Lors de la publication, le Préposé cantonal prend les mesures appropriées pour garantir la protection des données personnelles des parties.

- Recommandation du 19 janvier 2016 relative à ***une demande de M. D. en destruction de l'intégralité des documents d'une procédure pénale du Tribunal des mineurs***

  Cette requête était en relation avec une affaire au Tribunal des mineurs ayant fait l'objet d'un classement. Or, la personne concernée avait postulé pour entamer la formation de policier, ce qui l'avait amenée à signer un document autorisant la police à se renseigner auprès de toute institution pour obtenir des informations à son sujet. Estimant que le dossier concernant cette affaire pouvait potentiellement porter atteinte à ses intérêts, elle souhaitait sa destruction complète. Le Préposé cantonal a recommandé au Pouvoir judiciaire de ne ***pas répondre favorablement*** *à la requête visant à supprimer une procédure pénale archivée. Le*

calendrier de conservation relatif aux dossiers de procédure pénale du Tribunal des mineurs stipule que l'intégralité de la série doit être conservée, vu sa valeur archivistique. Les pièces de tous les dossiers doivent être conservées pour être ensuite versées aux Archives d'Etat. La base légale que constitue l'art. 6 LArch ne permet pas la destruction de la procédure pénale en cause et le Tribunal des mineurs ne peut pas la détruire. Le Préposé cantonal a aussi estimé que la requête ne relevait pas de sa compétence. Il a relevé, enfin, s'agissant de la question de l'accès aux pièces par des tiers, qu'au vu des règles sur le droit à l'oubli en droit pénal, une procédure de classement n'a pas à être communiquée à qui que ce soit, y compris à la police ou au Pouvoir judiciaire.
https://www.ge.ch/ppdt/doc/documentation/Recommandation-19-janvier-2016.pdf

Information donnée au Préposé cantonal en matière de traitement à des fins générales

A teneur de l'art. 41 al. 1 litt. e LIPAD, dans le cadre de l'accomplissement de leurs tâches légales, les institutions publiques sont en droit de traiter des données personnelles à des fins générales de statistique, de recherche scientifique, de planification ou d'évaluation de politiques publiques, pour leur propre compte ou celui d'une autre institution publique en ayant la mission légale, à la conditions notamment que le Préposé cantonal en soit préalablement informé avec les précisions utiles sur le traitement qu'il est prévu de faire des données personnelles et sa nécessité. En 2016, la Ville de Genève a informé le Préposé cantonal du souhait du Département de la culture et du sport de faire procéder à une enquête de satisfaction des usagers des bibliothèques municipales (horaires, prestations, etc.) auprès de 1'500 détenteurs d'une carte d'utilisateur. Ce processus implique la communication de données personnelles (nom, prénom, adresse) à une société privée, mandatée pour l'occasion. La liste des données transmises et les modalités de communication et de traitement de ces données ont fait l'objet d'un contrat de mandat, lequel a été transmis au Préposé cantonal, et qui prévoit notamment l'interdiction de sous-délégation, le traitement des données sur des serveurs sécurisés sis en Suisse et la destruction des données à la fin du mandat.

De quelques questions traitées ces derniers mois :

Les séances des commissions du Grand Conseil sont-elles publiques ?

A teneur de l'art. 9 LIPAD, sauf disposition légale contraire, les séances du bureau et des commissions et sous-commissions du Grand Conseil ne sont pas publiques. Le procès-verbal des séances des commissions approuvé est diffusé à tous les membres de la commission, aux députés qui ont remplacé un commissaire absent, aux conseillers d'Etat concernés et, sauf décision contraire de la commission, aux personnes qui assistent régulièrement à ses séances et travaux, aux autres députés, aux autres conseillers d'Etat et aux assistants politiques qui en font la demande. Il ne peut être communiqué à d'autres personnes que sur décision prise souverainement par la commission ou, pour les commissions dissoutes, par le bureau. Cette décision peut être assortie de charges et conditions. Elle n'est pas sujette à recours (art. 189 al. 5 et 6 LRGC).

La LIPAD prévoit-elle des facilités pour les journalistes s'agissant du droit à l'information ?

Oui, l'art. 31 LIPAD prévoit que les médias et les journalistes indépendants appelés à suivre régulièrement les affaires genevoises peuvent demander à recevoir à titre régulier et gratuit les documents faisant l'objet de délibérations publiques devant le Grand Conseil et les conseils municipaux ainsi que les informations mentionnées au chapitre II du titre II de la loi, dans la mesure où ces documents et informations ne sont pas rendus accessibles à un large public par le recours aux technologies modernes de diffusion de l'information. Par ailleurs, les institutions, compte tenu de leurs ressources, offrent aux médias et aux journalistes les facilités nécessaires à l'accomplissement de leur travail d'information, dans le respect du principe de l'égalité de traitement et dans les limites imposées par des contraintes objectives. Toutefois, la publicité d'une séance n'implique le droit pour les journalistes d'y effectuer des prises de vues et de sons et de la retransmettre que dans la mesure où le déroulement des débats ne s'en trouve pas perturbé et sous réserve des directives décrétées par l'institution considérée pour sauvegarder des intérêts légitimes prépondérants.

Une commune peut-elle indiquer sur son site Internet les noms de ses employés ?

Il est devenu habituel pour les communes de publier sur Internet, au titre de la communication active, les noms d'un certain nombre de leurs collaborateurs. Il est certes normal que les noms des responsables (secrétaire général, chef de service, directeur par exemple) soient publiés. Les règles sur la protection des données ne permettent toutefois pas de mentionner nominativement les autres employés sans leur

consentement. Le cas échéant, ces derniers peuvent tout à fait demander à ce que leur nom ne figure pas sur le site Internet. Notre autorité conseille donc de ne rendre publics que les noms des responsables. Pour les autres collaborateurs, seuls les numéros de téléphone doivent être indiqués.

Une commune peut-elle poser une webcam filmant des jardins sis sur le domaine public ?

Les art. 42 LIPAD et 16 RIPAD, qui contiennent des exigences strictes permettant le recours à de la vidéosurveillance, s'appliquent par analogie aux webcams. S'il ne s'agit pas de garantir la sécurité des jardins en prévenant la commission de déprédations, cela suscite déjà un problème quant au but envisagé. En outre, la LIPAD ne prévoit pas la diffusion des images, de sorte que les personnes entrant dans le champ de la caméra doivent avoir consenti au fait d'être filmées. A cet égard, la pose d'un panneau indiquant la présence d'une webcam est nécessaire, mais pas suffisante. Pour notre autorité, la conformité à la LIPAD implique que les personnes apparaissant dans le champ de la caméra ne doivent pas être reconnaissables.

~~~
~~~

~~~
~~~

Loi fédérale sur le dossier électronique du patient (LDEP)

En date du 22 mars 2016, le Département fédéral de l'intérieur (DFI) a ouvert l'audition relative aux ordonnances de la loi correspondante, qui durera jusqu'au 29 juin 2016. La loi fédérale sur le dossier électronique du patient fixe les conditions cadres pour le traitement des données et documents du dossier électronique du patient. Celui-ci vise à améliorer la qualité, la sécurité et l'efficacité des traitements médicaux, en accordant une priorité à la sécurité de l'information et à la protection des données. Outre rendre possible l'identification sans équivoque des patients, les ordonnances correspondantes règlent la certification des communautés concernées. Ces entités regroupent pour l'essentiel des cabinets médicaux, pharmacies, hôpitaux, organisations de soins à domicile et établissements médico-sociaux. Les ordonnances fixent par ailleurs les conditions-cadres pour l'attribution des aides financières pour la constitution et la certification de ces communautés. Une fois les ordonnances de mise en œuvre sous toit, la loi fédérale pourra entrer en vigueur en 2017. Rappelons que d'ici là, le canton de Genève doit procéder à quelques adaptations du dispositif genevois pour le mettre en conformité avec le nouveau droit fédéral à venir.

Casier judiciaire informatisé VOSTRA

Le 22 mars 2016, par 6 voix contre 2 et 1 abstention, la commission des affaires juridiques du Conseil des Etats a rejeté une disposition introduite par la Chambre du peuple lors de la dernière session, qui voulait que les auteurs de délits graves comme le meurtre, le viol, la prise d'otages ou des actes d'ordre sexuel sur des enfants ne bénéficient pas du droit à l'oubli en prévoyant que les jugements doivent rester dans VOSTRA jusqu'au décès du condamné. Pour la commission, seuls les jugements des personnes condamnées à la prison à vie doivent être inscrits dans VOSTRA jusqu'au décès de la personne. Dans tous les autres cas, les jugements devraient être biffés du casier judiciaire en fonction de leur gravité, entre 12 et 25 ans après la fin de la peine privative de liberté. Parmi les autres points de divergence, la commission a approuvé les autres décisions du National. Ainsi, les ordonnances de classement rendues par une autorité pénale ne figureront pas dans VOSTRA. Les députés estimaient que leur maintien dans le casier pouvait entacher la réputation d'une personne. Un des enjeux principaux de la révision de la loi sur le casier judiciaire informatisé VOSTRA visait à introduire un casier pour les entreprises. Le Conseil fédéral proposait d'y enregistrer les jugements pénaux et les procédures pénales. Mais le Parlement n'en veut pas et a enterré ce volet de la réforme, jugé inutile et coûteux par une majorité de droite. La nouvelle loi prévoit encore une extension massive des droits de consultation du casier. L'accès à VOSTRA sera accordé aux polices cantonales, aux autorités qui surveillent les placements d'enfants ou encore l'adoption internationale. Il est prévu de créer quatre extraits différents du casier, afin qu'une autorité ne connaisse que les informations absolument nécessaires pour accomplir ses tâches. Le dossier retourne au National.

~~~
~~~

les autorités pénales avaient dès le départ informé régulièrement sur l'avancement de l'enquête et que l'article contesté n'était paru que quelques mois après l'accident. De plus, tant les droits de la personnalité du prévenu que la présomption d'innocence avaient été violés. La publication de documents concernant les débats, pendant une procédure pénale, menaçait en outre le fonctionnement de la justice pénale.

Union européenne – Nouvelles dispositions européennes sur la protection des données

Les nouvelles dispositions européennes sur la protection des données, qui visent à rendre aux citoyens le contrôle de leurs données personnelles et à créer un niveau élevé et uniforme de protection des données à travers l'UE, adapté à l'ère numérique, ont reçu le feu vert final des députés européens le 14 avril 2016. Elles ont été publiées au Journal officiel de l'Union européenne le 4 mai 2016 (http://www.les-infostrateges.com/actu/16052183/publication-du-paquet-donnees-personnelles-au-joue). La réforme fixe également des normes minimales sur l'utilisation des données à des fins policières et judiciaires. Elle remplacera la directive actuelle sur la protection des données - qui date de 1995 alors qu'Internet était encore à ses débuts - par un *Règlement* général donnant aux citoyens plus de contrôle sur leurs propres informations privées dans un monde numérique de téléphones intelligents, de médias sociaux, de services bancaires sur Internet et de transferts mondiaux. Les nouvelles règles incluent des dispositions sur le droit à l'oubli; le consentement clair et explicite de la personne concernée quant à l'utilisation de ses données personnelles; le droit de transférer ses données vers un autre fournisseur de services; le droit d'être informé en cas de piratage des données; la garantie que les politiques relatives à la vie privée soient expliquées dans un langage clair et compréhensible; et une mise en œuvre plus stricte et des amendes allant jusqu'à 4% du chiffre d'affaires mondial total d'une entreprise, dans le but de décourager la violation des règles. Le paquet sur la protection des données inclut par ailleurs une *directive* relative aux transferts de données à des fins policières et judiciaires. La directive s'appliquera aux transferts de données à travers les frontières de l'UE et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre. Les nouvelles règles ont pour but de protéger les individus, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et limites clairs en matière de transferts de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales - incluant des garanties et des mesures de prévention contre les menaces à la sécurité publique, tout en facilitant une coopération plus aisée et plus efficace entre les autorités répressives. Le règlement entrera en vigueur 20 jours après sa publication au Journal officiel de l'UE. Ses dispositions seront directement applicables dans tous les États membres deux ans après cette date. Les pays de l'UE auront deux ans pour transposer les dispositions de la directive dans leur législation nationale.

Droit à l'oubli – Google fait appel

En date du 19 mai 2016, Google a annoncé engager un recours contre l'injonction de la France de déréférencer certains résultats de recherche sur toutes les extensions de son moteur de recherche. Le groupe américain porte ainsi devant la justice le débat sur la portée géographique du «droit à l'oubli». Google estime notamment que la Commission nationale de l'informatique et des libertés (CNIL), l'autorité française de contrôle en matière de données personnelles, n'a pas le pouvoir de l'obliger à faire appliquer ses décisions hors des frontières de l'Hexagone. L'affaire découle directement d'une décision de la Cour de justice de l'Union européenne (CJUE) qui a consacré le «droit à l'oubli» numérique en mai 2014. Grâce à ce «droit à l'oubli», les internautes résidant en Europe ont la possibilité d'obtenir des moteurs de recherche, comme Google ou Bing de Microsoft, le déréférencement d'informations les concernant sous certaines conditions. Leader mondial de la recherche sur Internet, Google a appliqué cette décision. Mais il limite les déréférencements aux versions européennes de ses sites comme google.fr en France, google.de en Allemagne ou google.ch en Suisse. La CNIL estime à l'opposé que la mesure, pour être efficace, doit s'appliquer à toutes les extensions géographiques et en particulier google.com. En février, le groupe américain a amendé sa pratique en appliquant un filtre sur toutes ses extensions. Ce dernier bloque l'accès aux contenus déréférencés, lorsqu'ils sont consultés depuis le pays où a été émise la demande de déréférencement. La mesure a été jugée insuffisante par la CNIL. Elle a prononcé en mars une sanction de 100'000 euros à son encontre.

~~~
~~~