



Newsletter

#01 / 2014

Chère lectrice, cher lecteur,

Depuis le mois de novembre 2013, j'ai le plaisir de présider la Commission cantonale de la transparence et de la protection des données. Comme l'indique son intitulé, dite Commission traite de deux missions distinctes, que d'aucun juge antinomique, soit la transparence et la protection des données.

Après quelques mois d'activité, j'ai pu constater que, au contraire, ces deux rôles sont interactifs et complémentaires. En effet, il m'appert que le droit à l'accès aux documents officiels et les exigences de la protection des données sont mieux garantis par une coordination assurée par une même commission.

Il n'est à cet égard pas vain de rappeler que la Loi cantonale du 9 septembre 2009 sur l'information et l'accès aux documents (LInf) fait clairement mention à la protection des données personnelles. Je pense entre autres aux articles 11 et 27 de la LInf.

Qui donc mieux qu'une autorité indépendante peut œuvrer au respect tant de l'information que de la sphère privée!

Respect, voilà un maître mot qui doit permettre à tout un chacun d'avoir confiance en l'information fournie.

En adressant récemment un message de bienvenue aux participants à la 7^e Journée suisse du droit de la protection des données, j'ai souligné qu'une forte augmentation des demandes d'installation d'un système de vidéosurveillance avec enregistrement a pu être constatée.

En effet, certainement lié au besoin accru de surveillance qui hante notre société, les systèmes de vidéosurveillance apparaissent comme la panacée. A ce titre, les préavis en ce domaine requis par la Loi cantonale du 7 décembre 2010 sur la vidéosurveillance qu'a émis la Préposée à la protection des données ont presque doublé en une année et ce en seulement deux ans d'application, passant de 28 à 48.

Il est dès lors à craindre que cela ne fera que s'amplifier à moins que le respect ne prenne le dessus sur le besoin de surveillance.

Je vous souhaite une agréable lecture.

Laurent Schneuwly,

Président de la Commission cantonale de la transparence et de la protection des données



ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Sommaire

Editorial	1
Actualités	2
Le principe de la transparence fête ses trois ans	2
«Cloud computing» en milieu scolaire	3
Impacts des autorités de surveillance	4
Deux conférences consacrées à «l'homme transparent»	5
Informations aux organes publics	7
Convention d'Aarhus	7
Révision d'un plan directeur communal	7
Facture d'eau du voisin	7
Rapport d'une commission	7
Communication de la liste des entreprises établies dans une commune	8
Communication des adresses des affiliés d'une caisse AVS à des entités	8
Communication d'images d'un accident enregistrées par une caméra de vidéosurveillance	8

Actualités

Le principe de la transparence fête ses trois ans

La Loi sur l'information et l'accès aux documents (LInf) est entrée en vigueur dans notre canton il y a trois ans. Le moment est venu de dresser un premier bilan. Un colloque destiné aux représentants des organes publics et aux journalistes a traité du principe de la transparence sous plusieurs angles.

Avant l'entrée en vigueur de la LInf, de nombreux organes publics craignaient une avalanche de demandes: l'évaluation des trois premières années révèle que tel n'a pas été le cas. Entre 40 et 50 demandes d'accès ont été enregistrées chaque année, a annoncé en préambule la Préposée à la transparence, Annette Zunzer Raemy. Ce n'est en aucun cas une avalanche, mais l'intérêt témoigné au droit d'accès est manifeste.

La Préposée à la transparence a estimé encourageant que la part des demandes d'accès ayant obtenu une réponse favorable ait augmenté la deuxième année avant de se stabiliser. D'après elle, le principe de la transparence semble s'être imposé auprès des organes publics. Les

documents relatifs aux domaines de l'environnement, des constructions et de l'administration ont suscité un intérêt particulier.

Un rapport d'audit fortement caviardé

Le secrétaire général de la Direction de l'économie et de l'emploi (DEE), Christophe Aegerter, a parlé de ses expériences dans le cadre de la première médiation suivant l'entrée en vigueur de la LInf. Il s'agissait d'un rapport d'audit du Service public de l'emploi, qui avait été commandé suite à des tensions internes en juillet 2010 et auquel les médias fribourgeois avaient demandé l'accès en mars 2011 à l'occasion d'une conférence de presse. Au vu de l'opposition de la plupart des tiers concernés, la DEE avait décidé en amont de la conférence de ne pas publier le rapport d'audit de manière proactive.

Suite aux demandes d'accès, la Direction avait repris contact avec les tiers concernés et proposé plusieurs caviardages au cours de la procédure pour que les médias puissent avoir au moins accès à une partie du rapport. La plupart de ces tiers s'y était opposé, sept d'entre eux avaient déposé une demande en médiation auprès de la

Préposée à la transparence en septembre 2011. Dans quatre cas, les parties étaient parvenues à une solution, alors que la Préposée avait finalement émis des recommandations dans les trois autres. Etant donné le risque d'atteinte grave aux droits de la personnalité des tiers concernés, elle avait recommandé des caviardages plus importants que prévu fin mars 2012¹.

A l'issue des autres étapes de la médiation et de la procédure interne au sein de la DEE, le rapport caviardé avait été remis aux requérants mi-mai 2013. Christophe Aegerter a souligné que la durée de la procédure ne s'est avérée satisfaisante pour aucune des parties impliquées. Et pourtant, on n'a cessé de constater tout au long du processus à quel point l'aspect psychologique de la médiation est important pour les tiers concernés.

Trop d'exceptions

Ce cas illustre clairement que le rythme de la procédure du droit d'accès ne correspond pas à celui du journalisme, a expliqué Philippe Castella, journaliste à La Liberté. Selon lui, les journalistes ont besoin d'informations rapidement, sans paperasserie aucune et non deux ans plus tard, sous une forme fortement caviardée qui plus est. C'est certainement une raison pour laquelle les journalistes recourent si peu au droit d'accès.

Malgré son nom, la loi sur l'information n'a pas été conçue pour les journalistes selon Philippe Castella: «C'est une loi qui règle essentiellement pour la population les questions de publicité des débats, d'information automatique et d'accès aux documents. Il y a juste quelques articles qui touchent directement les journalistes, mais qui pour la plupart entérinent des pratiques préexistantes». Le journaliste a lui-même pris part aux travaux préparatoires et s'est régulièrement trouvé en position minoritaire au sein du groupe de travail et, comme les autres journalistes,

s'est montré déçu du résultat final. A son avis, la loi prévoit bien trop d'exceptions avec une grande marge d'interprétation.

Arrêts en faveur de la transparence

A l'échelle suisse également, les interprétations des dérogations donnent lieu à toujours plus de recommandations du Préposé fédéral à la protection des données et à la transparence (PF PDT) et à des décisions judiciaires, a révélé Bertil Cottier, professeur à l'Université de Lugano. Ainsi, des commissions extraparlimentaires et des groupes de travail auraient souvent l'impression, à tort, de ne pas tomber sous le coup du principe de la transparence. En outre, les accords de confidentialité passés avec des tiers ne peuvent pas faire obstacle à la transparence.

Sur les sept arrêts que le Tribunal fédéral a rendus à ce jour dans ce domaine, six sont en faveur de la transparence.

En outre, la grande majorité des recommandations du PF PDT donnent pleinement ou partiellement raison aux requérants.

Un état d'esprit

Tant les conférenciers que les participants au colloque étaient d'accord sur le fait que le principe de la transparence constitue un état d'esprit. La tendance à la hausse depuis quelques années, dans le domaine de la communication proactive, est un signe positif. Reste à espérer que la population et les médias usent de plus en plus du droit d'accès et que cette tendance communicationnelle se renforce. A long terme, les éléments décisifs sont aussi bien le nombre de demandes d'accès que le sentiment des citoyens d'être informés sur l'activité de l'Etat et leur confiance envers les organes publics.

«Cloud computing» en milieu scolaire

Privatim, l'association des commissaires suisses à la protection des données, a convaincu la société Microsoft d'adapter ses dispositions contractuelles pour l'utilisation scolaire de son produit «Office 365». A cet effet, un complément contractuel a été élaboré afin d'assurer une utilisation conforme à la protection des données dans le milieu scolaire helvétique. Partant, la définition claire des responsabilités, le lieu du traitement des données (dans un pays européen), la définition d'instruments de contrôle suffisants, l'application du droit suisse ainsi qu'un for en Suisse font l'objet de ce complément contractuel.

¹ Cf. http://www.fr.ch/atprd/files/pdf43/Recommandation_du_26_mars_2012_-_Rapport_daudit.pdf

Impacts des autorités de surveillance

—
Le 31 mars 2014 s'est déroulé un séminaire sur la protection des données organisé par le Préposé à la protection des données du canton de Zürich en collaboration avec la «Zürcher Hochschule für Angewandte Wissenschaften» à Winterthur. Cette journée traitait des impacts réels de la surveillance de la protection des données, de son efficacité ainsi que des instruments à disposition des autorités de surveillance. Différents intervenants ont traité de la protection des données au niveau cantonal, fédéral, européen ainsi qu'international.

Il a été rappelé que les autorités cantonales de la transparence et de la protection des données sont des autorités entièrement indépendantes de surveillance et de conseil (non de décision). Ensuite, il a été souligné que la surveillance de la protection des données est efficace lorsqu'elle est effective et efficiente. Pour ce faire, chaque année, les autorités cantonales se donnent une liste d'objectifs à atteindre, en traitant de manière prioritaire et proactive des thèmes actuels, pour une mise en œuvre pratique de la protection des données.

Consolidation de la surveillance

Au niveau fédéral, l'Office fédéral de la justice propose une consolidation des compétences de surveillance du Préposé fédéral, un renforcement de son indépendance et une adaptation de la Loi sur la protection des données (LPD) par rapport aux challenges technologiques et sociaux actuels afin de consolider l'efficacité de la LPD. En effet, une extension des possibilités de sanction par le biais de décisions, d'amendes par exemple, un renforcement de l'indépendance du Préposé (externalisation du Bureau, autonomie du budget, activité à plein temps, interdiction d'occupation accessoire, élection par l'Assemblée fédérale) ainsi qu'une augmentation des ressources notamment par des financements alternatifs tels que des émoluments permettraient de rendre effective et efficiente la protection des données.

Evolution au niveau européen

Au niveau européen, la directive 95/46/CE est la pièce maîtresse de la législation en matière de protection des données à caractère personnel. Adoptée en 1995, elle

a pour objectifs de protéger le droit fondamental à la protection des données et de garantir la libre circulation des données à caractère personnel entre les Etats membres. Puis, elle a été complétée par la décision-cadre 2008/977/JAI destinée à protéger les données à caractère personnel dans les domaines de la coopération policière et de la coopération judiciaire en matière pénale. La rapide évolution des technologies a créé de nouveaux enjeux pour la protection des données à caractère personnel. Le partage et la collecte de données tant par les entreprises privées que par les pouvoirs publics ont connu une augmentation spectaculaire. Partant, les nouvelles technologies ont transformé l'économie et les rapports sociaux. Afin de mieux répondre aux défis posés par cette rapide évolution et par la mondialisation croissante, les membres de l'Union européenne réclament une plus grande sécurité juridique et une harmonisation plus poussée des règles en matière de protection des données à caractère personnel. Ainsi, afin de renforcer la dimension «marché intérieur» de la protection des données, de rendre l'exercice du droit à la protection des données par les personnes physiques plus effectif et d'instaurer un cadre global et cohérent couvrant tous les domaines de compétence de l'Union, y compris la coopération policière et la coopération judiciaire en matière pénale, la Commission européenne a proposé un ensemble de dispositions législatives répondant aux problèmes via le Règlement général sur la protection des données (Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données¹). Ce dernier n'entrera pas en vigueur avant 2017. Enfin, le projet Phaedra, qui vise l'expérience et les perspectives de la coopération relative à la protection des données entre les autorités européennes et internationales, a été présenté. Il ressort finalement que les sanctions inexistantes des autorités de surveillance, que le manque de ressource et que l'évolution constante de la société appellent à un changement pour une plus grande sécurité juridique et une harmonisation plus poussée des règles en matière de protection des données. Afin de pallier à ces manques, les autorités de surveillance doivent redoubler d'effort par la sensibilisation de la population et des organes publics et par la créativité.

¹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

Deux conférences consacrées à «l'homme transparent»

—
Sous le titre « L'homme transparent », deux conférences se sont tenues les 24 septembre et 29 octobre 2013 à Zurich à l'instigation du Pr Christiana Fountoulakis, professeur ordinaire à la Chaire de droit civil 1 de la Faculté de droit de l'Université de Fribourg, de la Paulus-Akademie de Zurich et de l'Association des dirigeants d'entreprise chrétiens en Suisse (VCU). Leur objectif était d'engager un dialogue public sur la transparence et la protection des données dans lequel s'expriment aussi bien les intérêts d'un accès maximal aux informations personnelles que les critiques et mises en garde.

Les conclusions de ces conférences de haut vol et dont la fréquentation fut très bonne peuvent se résumer comme suit: la notion d'«homme transparent» s'entend généralement dans un sens négatif, celui d'une radioscopie des sphères privées et intimes contre son gré. Pourtant, être «transparent», c'est-à-dire transparent sur le plan informatique, poursuit des buts tout à fait sensés, bien intentionnés ou du moins légitimement utiles. Etre surveillé par une caméra, par exemple, implique la divulgation d'informations, mais une surveillance (à bon escient) des espaces publics permet de limiter le nombre d'actes de violence et facilite leur poursuite (conférence du conseiller d'Etat Urs Hofmann). Malaise et méfiance vont habituellement de pair avec l'idée d'être un consommateur «transparent»; n'est-ce cependant pas positif si le commerçant connaît les préférences de son client et devient ainsi le coiffeur, boucher ou boulanger «de confiance», aux conseils et à l'offre duquel on peut se fier (conférence d'Alexander Meili)? D'aucuns sont aussi mal à l'aise à l'idée qu'un futur employeur ou une agence de placement soit au courant non seulement des qualifications professionnelles d'une personne, mais aussi de ses loisirs, de son voisinage et de ses relations familiales; ne s'agit-il pourtant pas d'informations que l'on rend soi-même publiques, sur les profils des réseaux professionnels et sociaux, sous forme de contributions sur les forums en ligne, etc. (conférence de Sabine Steinhorst)?

Transparence sans bornes

Le problème de la «nouvelle» transparence est qu'elle n'a pas de limites, du moins sur un plan technique. Voilà qui rend les technologies de l'information euphoriques, la protection des données pessimiste, et le citoyen et consom-

mateur très inquiet: la capacité de l'électrotechnique et de l'informatique à se procurer et à stocker les informations semble augmenter à l'infini. Sans compter les possibilités peu ou prou inépuisables de combiner les nombreuses informations autonomes qui rendent la personne concernée tout à fait «transparente» (et pas seulement au sens figuré; il suffit de penser à «google glass». Conférence du prof. Dirk Helbing).

Les acteurs non étatiques disposent aussi d'innombrables données sur les individus. C'est au plus tard depuis l'accès de Google Inc. à une position dominante sur le marché, proposant à la fois des services de moteur de recherche, de courrier électronique, un réseau social et un portail vidéo (YouTube), que les réserves à l'égard des entreprises privées se sont aussi manifestées: en utilisant de tels services Internet, le consommateur consent à ce que les sites consultés soient enregistrés et que son comportement sur Internet puisse être suivi. Même l'utilisation du mode navigation privée permet seulement d'éviter que le moteur de recherche n'enregistre des informations relatives à la page consultée; par contre, il n'est pas exclu que cette page, de son côté, n'enregistre des informations sur la visite. Qui ne souhaite pas que des informations soient stockées quant à ses habitudes de navigation, ne doit tout simplement pas recourir à de tels services informatiques. Et cette option semble presque inimaginable de nos jours.

Différences de sensibilité

Chacun ne montre pas le même degré d'inquiétude par rapport aux traces électroniques qu'il laisse chaque jour. Il y a un fossé culturel (juridique) entre les Etats-Unis, d'où viennent les entreprises Internet dominant le marché, et l'Europe (conférence du prof. Franz Werro). Alors qu'à l'échelle de l'Union européenne, il existe une proposition visant à renforcer le right to delete (droit de supprimer les données), en vertu de laquelle les informations qu'un particulier a rendues accessibles sur Internet peuvent être supprimées à certaines conditions¹, la formule *privacy is dead* (la vie privée, c'est fini) plaît non seulement aux représentants des technologies de l'information aux Etats-Unis mais aussi à de larges franges de la population qui l'acceptent comme une réalité peut-être importune, mais inévitable. Néanmoins, on peut identifier un phénomène qui dépasse l'Europe et les Etats-Unis et se résume par l'expression «génération Internet»: les jeunes s'inquiètent tout simplement moins de leur «autodétermination en

matière d'information» que les personnes plus âgées ; plusieurs études le révèlent, et on l'a aussi récemment constaté en Suisse².

Ce sont ensuite différents traits de l'être humain qui contribuent à la problématique de l'amoncellement des données («big data»), indépendamment de l'âge. La volonté d'être en permanente compétition, par exemple, entraîne automatiquement la divulgation d'informations. Le prof. Roberto Simanowski l'a montré dans sa conférence et a encore mentionné d'autres faiblesses qui incitent les personnes à laisser nonchalamment des traces électroniques: l'ignorance, l'avidité et la paresse. En ce sens, il est indispensable de se poser la question de la «véritable sphère privée» à l'ère d'Internet (conférence du prof. Markus Schefer). Ne peut-on pas penser que ce qui est publié n'est plus privé et ne doit par conséquent plus être protégé? On assiste en partie à une telle argumentation, mais elle est erronée du point de vue suisse. Laisser accessible à tous une information privée rendue un jour publique (p.ex., une photo d'enfance) peut tout autant porter atteinte à la personnalité que sa première publication. Comme souvent, il s'agit de procéder à une pesée des intérêts, entre l'intérêt au maintien de l'information du public et l'intérêt à la suppression de l'information en question³. Grosso modo, l'information privée doit être supprimée si elle n'est plus nécessaire pour le traitement des données – dans les limites du cadre légal.

Existence de bases légales

Par ailleurs, le Conseil fédéral a récemment refusé d'édicter des dispositions légales visant la protection de la sphère privée en lien avec Facebook, LinkedIn, etc.⁴. A juste titre: l'«homme transparent» évolue non seulement sur les sites Internet des réseaux sociaux, mais il est aussi citoyen, consommateur, employé, patient, assuré, etc.

Les lois spéciales relatives à un problème ponctuel sont souvent créées à la va-vite et insatisfaisantes en raison de leur champ d'application très restreint. Le rapport sur la nécessité de réviser la Loi suisse sur la protection des données⁵ révèle en outre que dans l'ensemble, le cadre légal permet aujourd'hui déjà de s'opposer aux abus en matière de traitement des données. Il est cependant effectivement vrai qu'en raison de la méconnaissance des moyens juridiques, rares sont les personnes à s'être défendues à ce jour contre l'intrusion non autorisée dans la sphère privée. Ainsi, la Loi sur la protection des données existe depuis 1995, mais la jurisprudence correspondante est encore insuffisante (l'arrêt relatif à «Google Street View» en 2012⁶ est un contre-exemple important); l'«offensive de charme» prévue afin de mieux faire comprendre à la population les outils légaux existants – mais peu utilisés à ce jour – doit y remédier. Il ne faut pas non plus oublier le programme national Jeunes et médias, lancé par le Conseil fédéral en 2010, qui vise notamment à montrer aux enfants, parents, enseignants et accompagnants comment avoir une utilisation raisonnable des médias numériques, c'est-à-dire en «minimisant les données».

Il incombe à la société d'adopter un comportement «discipliné en matière de données» – tant de la part du client ou du citoyen que de la part de l'opérateur de marché ou de l'Etat. D'un point de vue juridique, il s'agit principalement de veiller à une application efficace du droit à la non-collecte, non-transmission ou suppression des données personnelles, et ce sur un plan à la fois cantonal, national et international (pensons à l'accès aux pages Internet dans le monde entier), notamment par une application claire et uniforme de la question de la responsabilité civile et pénale en cas de traitement non autorisé des données ou d'atteinte à la personnalité⁷.

Prof. Christiana Fountoulakis

¹ Cf. proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) du 25.1.2012, COM (2012) 11 définitif, 2012/0011 (COD), art. 17. Voir aussi l'art. 12 let. b de l'actuelle Directive européenne sur la protection des données (95/46/CE); art. 15, al. 1, phrase 2 de la Loi fédérale sur la protection des données (LPD).

² Cf. NZZ du 11.12.2013, no 288, p. 13, qui fait référence à une enquête réalisée auprès de jeunes par l'IPMZ de l'Université de Zurich.

³ Cf. les art. 28 du code civil suisse (CC); art. 15 de la Loi fédérale sur la protection des données (LPD); voir aussi l'art. 12 de l'actuelle Directive européenne sur la protection des données (95/46/CE); art. 17 de la proposition de Règlement européen sur la protection des données.

⁴ Rapport du Conseil fédéral du 29.9.2011 en réponse au postulat Amherd 11.3912 «Donnons un cadre juridique aux médias sociaux».

⁵ Rapport du Conseil fédéral du 9.12.2011 sur l'évaluation de la Loi fédérale sur la protection des données, FF 2012 255.

⁶ ATF 138 III 346.

⁷ Cf. la jurisprudence différente en l'espèce in: Tribunal fédéral, 5A_792/2011 du 14.11.2013 (art. 28 s. CC); arrêt de la CJUE du 19.7.2011 l'Oréal / E-Bay, Rs C 324/09. Rec. I-6011 (art. 12 ss. de la Directive européenne sur le commerce électronique 2000/31/CE); conclusions de l'avocat général devant la CJUE in Rs C-131/12 Google Spain SL, Google Inc. c Agencia Española de Protección de Datos (Directive sur la protection des données 95/46/CE); arrêt de la CEDH du 10.10.2013 Delfi AS c Estonie (art. 10 CEDH).

Informations aux organes publics



Convention d'Aarhus

Depuis le 1^{er} juin 2014, les organes publics fédéraux et cantonaux doivent garantir un droit d'accès à l'information sur l'environnement, conforme à l'esprit de la Convention d'Aarhus. La Convention comprend trois piliers spécifiques: l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice. Dans le domaine du droit d'accès, plusieurs différences entre la Convention d'Aarhus et la Loi sur l'information et l'accès aux documents (LInf) sont à relever. Pour les documents environnementaux, le droit d'accès s'applique dorénavant sans limite de date. Dans le domaine de l'énergie nucléaire toutefois, la Suisse a émis une réserve. Seuls peuvent être consultés les documents postérieurs à l'entrée en vigueur de la Loi fédérale sur la transparence, c'est-à-dire les documents rédigés à partir du 1er juillet 2006. Le droit de consultation s'applique également aux particuliers ou aux corporations de droit public, qui se sont vus confier des tâches d'exécution dans le domaine de l'environnement. La Convention d'Aarhus et la Loi fédérale sur la protection de l'environnement actualisée sont accessibles sous les liens suivants:

<http://www.admin.ch/opc/fr/classified-compilation/20092191/index.html>

<http://www.admin.ch/opc/fr/classified-compilation/19830267/index.html>

Révision d'un plan directeur communal

Une commune, auprès de laquelle un citoyen avait sollicité l'accès au projet de révision du plan directeur et aux prises de position préalables, s'est renseignée auprès de notre autorité si elle devait accorder l'accès à tous ces documents. Elle considérait les prises de position comme des documents officiels et était disposée à les publier. Par contre, le projet de révision du plan directeur était d'après elle un instrument de travail pouvant encore subir des modifications. Comme il avait déjà été soumis à plusieurs services cantonaux pour avis, la Préposée à la transparence a plaidé pour sa mise à disposition.

Facture d'eau du voisin

Un habitant d'une commune a souhaité consulter la dernière facture d'eau de son voisin, sur quoi la commune s'est adressée à la Préposée à la transparence et a demandé si elle pouvait en accorder l'accès. Comme le compteur d'eau est contrôlé par un tiers sur mandat de la commune, qui établit ensuite la facture, la Préposée a considéré cette dernière comme un document officiel. Un tiers étant concerné par la demande, elle a signalé à la commune qu'il y avait lieu de consulter le voisin impliqué avant d'autoriser l'accès le cas échéant.

Rapport d'une commission

Une commune a pris contact avec la Préposée à la transparence après qu'une commission du conseil général eut demandé l'accès à un rapport élaboré par une autre commission à l'attention du conseil communal. La commission qui avait rédigé le rapport avait déjà donné son feu vert. La commune, en revanche, se demandait si l'accès devait effectivement être accordé, étant donné que le conseil communal ne s'était pas encore prononcé sur le rapport.

La Préposée à la transparence a répondu à la commune que l'organe public ayant rédigé le document demandé doit en principe traiter la demande d'accès. En ce sens, la commission compétente peut tout à fait accorder à ses collègues l'accès au rapport dans la mesure où aucune exception prévue par la LInf n'est applicable dans le cas concret.

Communication de la liste des entreprises établies dans une commune

—
Une entreprise nouvellement établie dans une commune a demandé la liste des entreprises déjà existantes à cette dernière. De manière générale, des données personnelles ne peuvent être communiquées que si une disposition légale le prévoit (art. 10 al. 1 LPrD). Dans ce cas d'espèce, aucune base légale ne prévoit que le Conseil communal puisse transmettre des données relatives aux entreprises établies dans sa commune. Cela étant, la Loi du 7 mars 2001 sur le Service du registre du commerce (LSRC) ainsi que l'Ordonnance du 17 octobre 2007 sur le registre du commerce (ORC) sont applicables, dans la mesure où le registre du commerce sert à la constitution et à l'identification des entités juridiques (art. 1 ORC). Selon l'article 10 ORC, «*les inscriptions au registre principal, les réquisitions et les pièces justificatives sont publiques*». Les cantons veillent à ce que les données du registre principal soient gratuitement accessibles sur Internet pour des consultations individuelles (art. 12 al. 1 ORC). Partant, le registre fribourgeois est tenu sur un support informatique et est public. Le canton de Fribourg veille à ce que les données de son registre principal soient gratuitement accessibles sur Internet et que les évolutions juridiques soient tenues à jour (art. 7 LSRC et art. 12 al. 1 ORC). Dans la mesure où le registre du commerce est public, chacun peut, sans avoir à justifier d'un intérêt particulier, consulter l'ensemble des inscriptions et des pièces justificatives. En conséquence, l'entreprise requérante peut s'informer auprès du Service du registre du commerce, notamment en accédant aux informations sur son site Internet.

Communication des adresses des affiliés d'une caisse AVS à des entités

—
Un citoyen s'est adressé à notre autorité pour savoir si une caisse AVS était habilitée à communiquer les adresses de ses affiliés à d'autres entités telles que les partis politiques et les écoles, dans le but de faire de la publicité. Selon l'art. 50a al. 1 let. bbis de la Loi du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS), «*dans la mesure où aucun intérêt privé prépondérant ne s'y oppose, les organes chargés d'appliquer la présente loi ou d'en contrôler ou surveiller l'application peuvent communiquer des données [...] aux organes d'une autre assurance sociale et d'autres services ou institutions habilités à utiliser le numéro AVS, si ces données sont nécessaires à l'attribution ou à la*

vérification de ce numéro». En outre, l'alinéa 4 précise que «*des données peuvent être communiquées à des tiers [...] b) s'agissant de données personnelles, lorsque la personne concernée y a, en l'espèce, consenti par écrit ou, s'il n'est pas possible d'obtenir son consentement, lorsque les circonstances permettent de présumer qu'il en va de l'intérêt de l'assuré*». En conséquence, la caisse AVS ne devrait pas communiquer les adresses de ses affiliés, d'une part, aux entités qui ne sont pas habilités à utiliser le numéro AVS et, d'autre part, si la communication des données n'est pas nécessaire à l'attribution ou à la vérification du numéro AVS. Par ailleurs, le consentement de la personne concernée est nécessaire dans les cas où la communication de données personnelles à des tiers n'est pas expressément autorisée.

Communication d'images d'un accident enregistrées par une caméra de vidéosurveillance

—
L'autorité a été saisie d'une question concernant la communication d'images d'un accident, enregistrées par une caméra de vidéosurveillance installée sur une route cantonale, à l'assureur responsabilité-civile privé d'un des conducteurs. L'autorité est arrivée à la conclusion qu'il n'est pas admissible de communiquer les images de l'accident selon le principe de la finalité (art. 5 LPrD). En effet, la communication des images ne correspond pas au but de l'installation de la caméra qui a enregistré l'accident. Conformément à l'art 22 al. 1 du Règlement du 7 décembre 1992 d'exécution de la loi sur les routes (RELR, RSF 741.11), les caractéristiques techniques des routes et des ouvrages annexes sont définies dans les normes de l'Union suisse des professionnels de la route (normes VSS). Les normes VSS qui prescrivent l'installation des caméras vidéo sur les routes ont pour but la surveillance du trafic, mais pas la détection des accidents de la route. Le but de l'assureur étant plutôt de nature économique, à savoir le degré de responsabilité civile de son assuré et ainsi de déterminer le montant du dommage qu'il doit verser, la communication des images n'est dès lors pas possible. L'autorité a aussi jugé que l'accès aux images de l'accident par l'assureur n'était pas conforme au principe de la bonne foi. En effet, il n'est pas possible d'exiger des usagers de la route qu'ils s'attendent à ce que les images des caméras routières, installées dans le but de surveiller le trafic routier et régies dans les normes privées VSS, puissent être utilisées par des assureurs privés à des fins économiques.



Autorité cantonale de la transparence et de la protection des données ATPrD

Rue des Chanoines 2, CH-1700 Fribourg

T. +41 26 322 50 08, F + 41 26 305 59 72

-

www.fr.ch/atprd

-

Juin 2014