# Newsletter
## #01 / 2015

Chère lectrice, cher lecteur,
«Big Data» et droit de la protection des données: le thème choisi pour la 8e journée suisse du droit de la protection des données était non seulement vaste, mais également ambitieux.
En effet, comme sa définition l'indique, les «Big Data», littéralement les «grosses données» ou mégadonnées, désignent des ensembles de données qui sont tellement volumineux qu'ils en deviennent difficiles à travailler avec des outils classiques de gestion de base de données ou de gestion de l'information. Dans ces nouveaux ordres de grandeur, la capture, le stockage, la recherche, le partage, l'analyse et la visualisation des données nécessitent d'être redéfinis. Les perspectives du traitement des «Big Data» sont énormes et pour partie insoupçonnées.
Divers experts, institutions, administrations et spécialistes considèrent ce phénomène comme l'un des grands défis informatiques de la décennie 2010-2020 et en ont fait une de leurs nouvelles priorités de recherche et de développement. C'est à ce phénomène que se sont attaquées les conférences données le 29 mai dernier à l'Université de Fribourg.
Les risques auxquels nous sommes et serons encore confrontés ressortissent aux enjeux inhérents à la croissance des données définis par d'aucun comme étant tridimensionnels et répondant à la règle dite des «3 V», soit volume, vélocité et variété.
Si les volumes sont véritablement en pleine expansion, les installations produisant de plus en plus de données, leur variété et leur vélocité, à savoir la fréquence à laquelle les données sont générées, capturées et partagées, sont générateurs d'enjeux colossaux.
Pour s'en convaincre, il suffit de relever que, depuis l'année 2012, le Département de la défense américain investit annuellement plus de 250 millions de dollars sur les projets des «Big Data» et que leur analyse a joué un rôle important dans la campagne de réélection de Barack Obama, entre autres pour analyser les opinions politiques de la population. La National Security Agency, plus communément connue sous NSA, l'a également compris puisque construisant un centre permettant de collecter toutes les données Internet qu'elle réunit.
Le secteur privé n'est pas en reste comme le témoignent notamment le million de transactions clients par heure traités par Walmart et les 50 milliards de photos traités par Facebook. Ce phénomène va encore s'accélérer de par l'explosion du marché des supports mobiles (smartphones et tablettes notamment) et à la démocratisation du cloud-computing grâce à des outils comme Dropbox.
A la lecture de ces quelques lignes, vous aurez compris que, confrontée aux «Big Data», la protection des données va devoir affronter des défis tout autant insoupçonnés que majeurs.
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

EC 902

# Sommaire



# Actualités

## «Big Data» et droit de la protection des données

*La 8e Journée suisse du droit de la protection des données a permis d'aborder le thème des «Big Data» de divers points de vue. Les nombreux orateurs ont analysé ce concept et la problématique liée à ce phénomène ainsi que les défis qu'il pose au droit de la protection des données.*

Un constat général ressort des exposés et des discussions: le système juridique actuel est inefficace face aux «Big Data», terme désignant une grande quantité de données provenant de diverses sources, saisies et enregistrées par des moyens permettant une vitesse de traitement élevée pour être ensuite évaluées et analysées à des fins et pour une durée indéterminées. Diverses solutions ont été proposées, prévoyant parfois d'abandonner certaines règles liées à la protection des données. D'autres propositions préconisent un élargissement du droit de la protection et cela également en dehors du secteur public (recours collectifs, transparence sur les recoupements de données ou les algorithmes).

Un problème fondamental posé par les «Big Data», du point de vue de la protection des données, réside dans le fait qu'un ensemble de données anonymisé ne paraît souvent pas problématique au premier abord, puisqu'il n'est pas possible d'établir un lien avec un individu précis. Toutefois, si de grandes quantités de données sont croisées, il se peut que des données initialement anonymisées puissent malgré tout être rattachées à une personne. Un autre problème est que de grandes quantités de données, dont l'Etat peut disposer aujourd'hui, sont prélevées sans intervention des personnes concernées. Le droit fondamental à la préservation de la sphère privée requiert un traitement plus consciencieux des données, notamment en indiquant dans quel but celles-ci seront utilisées.

Les intervenants ont eux-mêmes reconnu que surtout les préposés à la protection des données et les juristes en général sont conscients de l'importance de cette problématique. Néanmoins, la majorité de la population ne la perçoit pas de la même manière. Il suffit pour s'en rendre compte de penser au nombre de personnes qui mettent en ligne des données personnelles sensibles sur Internet, sans voir aucun problème à cela.

## Accès aux informations et protection des données

—

*Accès aux informations et protection des données – une tension insurmontable? Des représentantes et représentants de privatim, l'association des commissaires suisses à la protection des données, se sont penchés sur cette question début mai à Baden, en compagnie de spécialistes des autorités judiciaires, des archives, de la statistique et d'autres domaines.*

Après un exposé sur le caractère public des ordonnances pénales et des décisions de non-lieu, présenté par M. Christian Aebi, Procureur général du canton de Zoug, il a surtout été question des «*Open Government Data*». Mme Anne Wiedmer, des Archives fédérales suisses, a présenté la stratégie de la Confédération dans ce domaine (www.opendata.admin.ch).

Mme Wiedmer a ainsi expliqué que l'approche de la Confédération en la matière consiste à rendre accessible au public le plus de données administratives possible, pour autant que la publication de ces données n'enfreigne pas le droit en vigueur. Les effets attendus sont l'innovation et la croissance économique, la transparence et la participation ainsi qu'une efficience accrue de l'administration. Selon elle, la prudence s'impose toutefois, notamment en lien avec des données personnelles particulièrement sensibles. En effet, de nombreuses données techniques ont aussi un caractère personnel et la manière de procéder en présence de données personnelles particulièrement sensibles est, en conséquence, précisément définie.

### Supprimer durablement le caractère personnel des données

M. Beat Rudin, Préposé à la protection des données du canton de Bâle-Ville, souligne que les exemples d'application sont très nombreux. Ainsi, des données relatives aux emplacements des toilettes publiques comportant une table à langer, à l'utilisation des recettes fiscales, aux lieux propices aux accidents ou encore des données météorologiques ont pu être regroupées ou pourraient l'être.
Tout le monde s'accorde sur le fait que les «*Open Government Data*» ne sont pas des informations à caractère personnel, puisque tout lien éventuel avec une personne doit être supprimé en anonymisant les données. Cependant, tout le monde s'accorde-t-il également sur ce que sont exactement des données à caractère personnel ? En effet, comme le fait observer M. Rudin, les personnes concernées peuvent être identifiées non seulement par leur nom, mais également, de manière indirecte, au moyen du contexte, par exemple par géoréférencement. On peut donc uniquement parler d'une anonymisation correcte des données lorsque leur caractère personnel a été durablement supprimé.

### Problème des «Big Data»

Dans le cas des «Big Data», un défi supplémentaire entre en ligne de compte. Selon M. Beat Rudin, la combinaison de différentes données personnelles qui ont toutes été correctement anonymisées, provenant de différentes sources, peut permettre de retracer leur lien avec les personnes concernées. Il est donc nécessaire de se demander si le risque de «désanonymisation» dans le domaine des «*Open Government Data*» peut être éliminé.

***privatim*** *est l'association des commissaires suisses à la protection des données. Elle a pour but, par la collaboration et l'échange d'informations, de conférer plus d'importance aux intérêts de la protection des données et de faire un usage plus efficient des ressources. privatim est un interlocuteur pour les autorités et le public. Vous trouverez d'intéressantes publications sous www.privatim.ch, rubriques «Publications» et «Conférences», sous lesquelles les présentations de la conférence mentionnée ci-dessus peuvent être téléchargées.*

## Le Conseil fédéral donne le mandat de révision de la LPD et de la LTrans

—

*Le Conseil fédéral a chargé le Département fédéral de justice et police d'une révision de la Loi sur la protection des données. Il a donné également le coup d'envoi d'une révision partielle de la Loi sur la transparence.*

Avec la révision partielle de la Loi sur la transparence (LTrans), le Conseil fédéral (CF) veut améliorer la mise en œuvre du principe de la transparence dans l'administration fédérale. Un groupe de travail interdépartemental sera par ailleurs institué, qui assurera les échanges au sein de l'administration fédérale.
Le nombre des demandes d'accès à des documents officiels qui se fondent sur la LTrans a considérablement augmenté ces dernières années, entraînant certains problèmes de mise en œuvre. A titre d'exemple, les entreprises dont les secrets d'affaires et de fabrication sont ou pourraient être concernés par des demandes d'accès ne sont aujourd'hui pas suffisamment impliquées dans la procédure. Par crainte de procédures possibles pour atteinte au secret commercial, les autorités se montrent souvent réservées envers l'accès à des documents officiels. La révision partielle de la LTrans doit permettre de trouver de nouvelles solutions.
Le CF a également chargé le Département fédéral de justice et police (DFJP) d'examiner des options pour raccourcir la procédure de médiation et de réfléchir à la manière de clarifier les rapports entre protection des données et LTrans.

### Renforcement de la protection des données

Dans le domaine de la protection des données, le CF a chargé le DFJP de lui soumettre un avant-projet d'ici à fin août 2016, tenant compte des réformes en cours dans l'UE et au Conseil de l'Europe. La révision de la Loi sur la protection des données (LPD) devrait mettre la Suisse en état de ratifier la nouvelle convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de reprendre si nécessaire les développements de l'acquis de Schengen/Dublin en matière de protection des données. Pour faire mieux appliquer la loi, il convient d'examiner s'il ne serait pas opportun de renforcer non seulement les attributions et les pouvoirs du Préposé fédéral à la protection des données et à la transparence, mais aussi, ponctuellement, les droits des personnes concernées et la procédure qu'elles doivent suivre pour les faire appliquer. La question est d'intérêt notamment dans les domaines où le droit suisse présente des lacunes par rapport aux réformes du Conseil de l'Europe.
Le Conseil fédéral entend aussi améliorer le contrôle et la maîtrise des données, de même que la protection des mineurs. Enfin, il souhaite que la protection des données soit assurée plus en amont, grâce à la promotion de bonnes pratiques.

### Le changement de paradigme a-t-il eu lieu?

—

A l'initiative de la Conférence des secrétaires généraux de l'administration fédérale, la LTrans a été évaluée l'an passé. Il s'agissait de déterminer, notamment, si le changement de paradigme – du principe du secret au principe de la transparence – avait eu lieu dans l'administration fédérale.

Les utilisateurs considèrent la LTrans comme un moyen de contrôler le travail des autorités et se montrent plutôt sceptiques envers le succès de la mutation. Le tableau de la situation n'est toutefois pas uniforme: la majorité des autorités ont procédé à une certaine réforme culturelle, une minorité pas encore. Les autorités examinées sont néanmoins en mesure d'appliquer le principe de la transparence.

L'évaluation a par ailleurs montré que les ressources du Préposé fédéral à la protection des données et à la transparence (PFPDT) sont insuffisantes dans le domaine de la transparence. Toujours selon l'évaluation, la procédure de médiation devant le PFPDT est trop longue. Les requérants jugent cependant la procédure de médiation de manière très positive et les recommandations du PFPDT sont généralement très bien accueillies, notamment auprès des requérants.

L'analyse juridique démontre que les recommandations du PFPDT sont soutenues par les tribunaux et qu'il n'existe pour l'instant aucun jugement valable s'écartant notablement des recommandations. 90% des procédures de médiation menées par le Préposé n'entraînent aucune procédure judiciaire.

## Droit à l'oubli – du Mythe à la Réalité

—

*Un colloque, à l'Université de Lausanne, a mis en lumière un thème très actuel – le droit à l'oubli – sous différentes perspectives: européenne, suisse, technologique, journalistique et alternative. La raison de l'engouement du public face à cette notion est l'arrêt de la Cour de Justice de l'Union Européenne (CJUE) du 13 mai 2014 dans l'affaire opposant la Commission à l'Espagne (affaire C 184/11), plus communément appelé «l'arrêt Google». Et comme le mentionne le titre du colloque organisé par le Centre du droit de l'entreprise de l'Université de Lausanne (CEDIDAC), le sujet porte sur l'existence réelle ou non de ce «droit».*

Aujourd'hui, le droit à l'oubli ne laisse plus personne indifférent. Alors que bons nombres d'individus ne cessent d'invoquer ce droit, depuis l'arrêt Google et la réaction de Google par la mise en place de formulaires de droit à l'oubli, peut-on véritablement définir les enjeux et la portée de ce «droit»? Jean-Philippe Walter, Préposé fédéral suppléant à la protection des données et à la transparence, explique que selon la perspective européenne l'arrêt Google, dans lequel la Cour répond à une demande de décision préjudicielle de l'Espagne suite à une décision de l'Agence espagnole de la protection des données ordonnant à Google de prendre les mesures nécessaires pour retirer les données d'un plaignant de son index et d'empêcher l'accès à ses données à l'avenir, consacre non un droit à l'oubli, mais un droit au déréférencement ou à la désindexation sur les moteurs de recherche.

### Pondération des intérêts

Mais le droit à l'oubli, c'est quoi? D'après la perspective suisse, présentée par le Professeur Philippe Meier, Professeur à l'Université de Lausanne et avocat, la réponse est simple: le «droit à l'oubli» est une notion impropre qui exprime une situation ou un état auquel l'individu aspire, c'est-à-dire ne plus voir des informations le concernant dans les médias, dans des ouvrages, etc. Il précise ainsi qu'en tant que tel le droit à l'oubli n'existe pas, mais reflète uniquement un état recherché «être oublié».

Il explique qu'en se référant aux différentes décisions rendues par les tribunaux ainsi qu'à la volumineuse doctrine basée sur l'art. 28 Code Civil, disposition générale sur la protection de la personnalité, une définition quelque peu classique peut être donnée. Ainsi, le droit à l'oubli serait un «droit à la non-(ré)évocation». Ce droit, comme tous les droits de la personnalité, n'est pas absolu et il doit être pondéré avec d'autres droits ou intérêts légitimes. Il revêt, toutefois, plusieurs aspects, à savoir le droit de ne pas être recherché par son nom, le droit de correction ou de suppression de données, le devoir de traiter des données exactes, la conservation limitée dans le temps des informations et le droit d'opposition.

Au final, il est question du droit relatif et imprévisible d'une personne à ne plus voir des informations la concernant ressurgir après un certain temps alors que l'actualité ne le justifie aucunement. L'aspect imprévisible repose sur le fait que le droit à l'oubli est analysé au cas par cas et est mis en balance avec les différents intérêts en présence.

Le Professeur Jean-Henry Morin, professeur à l'Université de Genève, déclare que le droit à l'oubli est «une mauvaise réponse à une question mal posée». Du point de vue technique ou technologique, il s'agit plutôt d'examiner la possibilité de concevoir des systèmes et des services capables de répondre à ce besoin. D'après lui, tout est techniquement réalisable: seul le contexte et le temps sont des facteurs d'influence.

### Balance est importante

Du côté des médias, comme les droits protégeant la personnalité, la liberté d'informations doit être pondérée: c'est-à-dire une balance entre l'intérêt du particulier à ce que l'information ou l'événement soit passé sous silence, voire non-réévoqué, et l'intérêt du public à être informé doit être faite. Dès lors, il y a différentes manières pratiques d'aborder le droit à l'oubli. Une assez grande palette d'actions est envisageable face à la proéminence d'informations librement accessibles. Ils peuvent ne rien faire, anonymiser l'article, déréférencer l'article (cf. formulaire Google) ou encore simplement supprimer l'article.

Les journalistes et les autres professionnels du domaine sont bien évidemment soumis au système législatif, et plus particulièrement à des règles déontologiques et des directives édictées par le Conseil de la Presse suisse. Le critère central est certainement l'écoulement du temps analysé sur la base de la pertinence actuelle de l'information, la nature de l'information, la qualité que

revêt la personne concernée, etc. Me Gianni Cattaneo ajoute que face aux médias, invoquer le droit à l'oubli peut entraîner l'effet inverse – effet Streisand – médiatisation involontaire de l'information que l'on souhaiterait faire disparaître, comme cela a été le cas dans l'affaire Google.

Partant, le droit à l'oubli est une réponse aux besoins de protection de l'individu nés de l'essor des nouvelles technologies, des changements de mœurs notamment l'éphémérité des échanges, d'une soif quelque peu inexpliquée de partager tous les moments qui constituent notre quotidien, mais également d'une rupture de confiance massive envers l'informatique et d'un trop plein d'informations. Il ressort de ce colloque que le droit à l'oubli n'existe qu'au travers d'autres droits notamment les droits protégeant la personnalité et ne peut être invoqué qu'à certaines conditions.

# Informations aux organes publics

## Accès à la boîte mail

Une commune a saisi notre Autorité afin de savoir si elle est en droit, en tant qu'employeur, d'accéder au contenu de la boîte mail de son employé. A titre préliminaire, il est nécessaire de vérifier si la commune possède son propre Règlement relatif au personnel communal. A défaut, la Loi sur le personnel de l'Etat de Fribourg (LPers) ainsi que les Ordonnances et Règlements y relatifs lui seraient applicables. Dans le cas d'espèce, en absence de Règlement communal, l'Ordonnance du 20 août 2002 relative à la surveillance de l'utilisation d'Internet par le personnel de l'Etat (ci-après: Ordonnance) est applicable au personnel communal. En effet, l'utilisation d'Internet recouvre l'accès à Internet et à Intranet, y compris le courrier électronique et les médias sociaux (art. 1 al. 2 de l'Ordonnance). En principe, l'usage d'Internet au travail est réservé à des fins professionnelles. Toutefois, son utilisation occasionnelle à des fins privées, y compris celle du courrier électronique et des médias sociaux, est tolérée dans les limites résultant de l'obligation de service de consacrer tout son temps à son travail. Lorsqu'il y a des indices d'abus, des contrôles personnalisés peuvent être ordonnés par le Syndic de la commune et exécutés par le Service ou l'unité informatique compétente. Toutefois, en ce qui concerne le courrier électronique, le contrôle se limite au nombre de messages envoyés et reçus, aux éléments d'adressage, aux types et volumes de fichiers attachés; il ne porte pas sur le contenu des messages. Ainsi, en cas d'abus, le Syndic de la commune doit entendre le collaborateur et s'il s'avère que l'abus constitue une violation des devoirs de service, ce dernier prendra alors les mesures appropriées conformément à la législation sur le personnel de l'Etat. Il est nécessaire de rappeler qu'en aucun cas le contenu des mails ne pourra être lu par l'employeur sauf si la personne concernée y a consenti.

## Consultation de procès-verbaux communaux

Plusieurs communes du canton de Fribourg ont abordé notre Autorité afin de savoir s'il est admissible, du point de vue de la protection des données, qu'elles autorisent la consultation de leurs procès-verbaux à un particulier. De cette question découle deux cas de figures: le droit d'accès du public aux documents officiels et le droit d'accès de la personne concernée aux données la concernant.

Aux termes de la Loi sur l'information et l'accès aux documents, toute personne a le droit d'accéder aux documents officiels détenus par les organes publics et ce dans la mesure prévue par la loi (art. 20 al. 1 LInf). Cependant, l'accès aux procès-verbaux des séances non publiques, telles que les séances du Conseil communal, n'est pas garanti (art. 29 al. 1 let. b LInf). La Loi sur les communes prévoit à son art. 103bis al. 2 let. a que le conseil communal peut autoriser, par une décision prise à l'unanimité, la consultation de tout ou partie des procès-verbaux de ses séances, des séances des commissions de l'assemblée communale et des séances de commissions administratives. Conformément au principe de la proportionnalité, il convient alors de caviarder les éventuelles données personnelles concernant des tiers.

En matière de protection des données, le droit d'accès est un droit au renseignement qui permet à toute personne de demander au responsable d'un fichier si des données la concernant y sont traitées, et le cas échéant les consulter (art. 23 LPrD). Toutefois, ce droit n'est pas absolu et peut être limité pour la sauvegarde d'intérêt public prépondérant, dans l'intérêt d'un particulier, voire même dans l'intérêt du requérant lui-même (cf. art. 25 LPrD). Ainsi, le Conseil communal communiquera à la personne concernée toutes les données la concernant qui sont contenues dans les procès-verbaux et ce dans les limites de la loi. Pour ce faire, les documents devront être anonymisés et seules les parties concernant le requérant pourront être communiquées.

## Surveillance du poste de travail d'un collaborateur

—

La surveillance du poste de travail de son employé est une question récurrente posée à notre Autorité. A titre préliminaire, la surveillance des travailleurs n'est pas régie par une seule norme, mais par plusieurs lois dont les principes ont été complétés par la pratique des tribunaux, mais surtout par des directives et des recommandations, telles que celles du Préposé fédéral à la protection des données (http://www.edoeb.admin.ch) et celles du Secrétariat d'Etat à l'économie (http://www.seco.admin.ch). L'installation d'un système de surveillance sur le poste de travail d'un employé se doit de respecter non seulement les droits fondamentaux (vie privée et liberté personnelle), mais également les principes généraux de la protection des données (légalité, finalité, bonne foi, exactitude et proportionnalité) et finalement la protection des travailleurs, afin de trouver un équilibre entre l'intérêt à la bonne exécution du travail et au respect des directives de l'employeur, et la protection de la sphère privée du travailleur. Tout employeur qui envisage une surveillance de ses employés devrait les informer préalablement et de manière transparente, dans un règlement d'utilisation et de surveillance, de la manière dont la surveillance est exercée, dans quel but elle est menée ainsi que des droits et obligations qui leur échoient. En application du principe de proportionnalité, l'employeur recourra principalement à des contrôles anonymisés et si besoin par sondage à des contrôles sur une base pseudonymisée (non nominale). Un contrôle nominatif ne devrait avoir lieu qu'en cas de soupçons fondés. En outre, il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail; exception faite des autres motifs (cf. art. 26 de l'Ordonnance 3 relative à la loi sur le travail) où les employés devront être complètement informés et la mesure proportionnée.

## Adaptation de la Loi sur l'information et l'accès aux documents

—

L'avant-projet de loi modifiant la loi sur l'information et l'accès aux documents (LInf) a été mis en consultation. La loi doit être adaptée à la Convention d'Aarhus, entrée en vigueur pour notre pays le 1er juin 2014. La Convention d'Aarhus octroie au public un droit d'accès aux documents environnementaux qui va plus loin que celui qui est prévu de manière générale par la LInf. Il existe donc certaines incompatibilités entre la LInf et la Convention, qu'il convient de résoudre. Deux variantes sont soumises, le délai de consultation dure jusqu'à mi-septembre.

**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 2015