



Newsletter

#02 / 2012

La protection des données aujourd'hui

La protection des données dans l'administration publique, c'est la protection de la personne, la protection de ses droits fondamentaux.

Avant la législation sur la protection des données, la circulation des informations personnelles était fermée envers le citoyen et ouverte au sein de l'administration publique. La loi de 1994 sur la protection des données a inversé les paradigmes. L'un des rôles de la Préposée à la protection des données a été de dire: ouverture envers l'administré (droit d'accès à ses propres informations) et secret en interne lorsqu'il n'y a ni obligation légale, ni nécessité pour l'accomplissement de la tâche de communiquer les informations sur des personnes individuelles.

20 ans après, on s'est rendu compte que l'administration publique ne peut pas être ouverte que pour la personne individuelle par rapport à ses données personnelles, mais qu'elle doit l'être pour le public en général. Le législateur a voulu renforcer la transparence, l'autre face de la médaille, et l'étendre à l'ensemble de l'activité administrative.

On pourrait voir une contradiction entre «transparence» et «protection des données personnelles». Ce n'en est pas une. La transparence de l'activité de l'Etat a trait justement à son activité en général, alors que la protection des données s'applique lorsque les droits fondamentaux de la personne sont touchés ou pourraient l'être. Ce n'est pas le même objet, il s'agit de l'activité de l'Etat et pas de celle des personnes individuelles.

Mais quels sont ces droits fondamentaux? L'art. 12 de la Constitution cantonale dispose que toute personne a droit au respect de sa *vie privée et familiale, de son domicile, de sa correspondance et de ses télécommunications*. Elle a le droit d'être protégée contre l'usage abusif de ses propres données. Cela signifie que l'administration publique ne peut pas agir sans limites avec les informations personnelles qu'elle détient. L'être humain n'est pas un objet que l'on se passe d'un endroit à l'autre de l'administration publique, ses données personnelles doivent être traitées avec retenue. Le respect de la personne est un élément clé de la confiance de l'individu envers ses autorités et cette confiance est indispensable au bon fonctionnement de notre démocratie.

Dominique Nouveau Stoffel
Préposée à 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
<hr/>	
Actualités	2
Transparence, protection des données et sphère privée: un rapport complexe	2
Contrôle des webcams du canton de Fribourg	3
La médiation, une voie vers la résolution d'un conflit	4
<hr/>	
Informations aux organes publics	5
Recommandation sur l'accès à un rapport technique	5
Droit d'accès à son dossier médical	5
Communication d'une liste de nouveau-nés à une bibliothèque communale	5
Communication électronique de données d'aide sociale	6
Utilisation des offres «cloud» dans le contexte scolaire	6
Publication de photos des enfants des écoles	6
Arrêt de la CJUE du 16 octobre 2012 - Commission européenne contre la République d'Autriche	7
<hr/>	

Actualités

Transparence, protection des données et sphère privée: un rapport complexe

Ces derniers temps, le rapport entre la transparence et la protection de la sphère privée est apparu comme l'un des principaux thèmes en lien avec l'évolution de la société de l'information. Des discussions intenses, de nature philosophique notamment, se tiennent actuellement dans les médias. Un symposium a abordé cette problématique à Berlin à l'occasion de la Journée internationale du droit d'accès à l'information du 28 septembre.

Entre ceux qui défendent l'idée d'une ère de 'post privacy' et ceux qui dénoncent les dangers d'une société de la transparence, chacun a décrit son point de vue à Berlin et a alimenté la discussion. Dans quelle mesure un Etat ou une organisation peuvent-ils prôner la transparence? Une transparence totale est-elle au fond souhaitable? Peut-on encore garantir à l'individu le respect de sa sphère privée?

«Un bon Etat n'a pas de secrets»

La transparence représente l'absence de secrets, a déclaré Alexander Morlang, député du Parti pirate allemand. D'après lui, les secrets pourraient sceller des rapports de force: «Si l'on n'est pas au courant, on ne peut pas prendre part à la discussion. Si l'on ne peut pas prendre part à la discussion, on n'est pas de la partie.» Il pense comme le sociologue Georg Simmel, qui a dit il y a près de cent ans qu'un bon Etat n'avait pas de secrets.

Selon Alexander Morlang, le propre travail politique du Parti pirate montre aussi que la revendication d'une transparence absolue est souvent dangereuse. Pour lui, elle entraîne des dérobades, des décisions ne sont par exemple plus prises lors de séances publiques. Dans de nombreux cas, il estime nécessaire de remplacer une transparence en temps réel par une transparence dans le temps. «Si la transparence est obtenue de force de manière importune, elle peut mener à la paralysie», a-t-il conclu avec conviction.

Internet n'oublie rien

La problématique entre la protection des données et la liberté d'information est régulièrement abordée dans la jurisprudence. Hans-Hermann Schild, président du Tribunal administratif de Wiesbaden, a par exemple cité un arrêt de la Cour de justice de l'Union européenne portant sur le degré de transparence dans le cadre de la publication sur Internet des subventions du Fonds européen agricole.

La Cour a émis de sérieux doutes quant à la nécessité de publier le nom des personnes physiques bénéficiant de subventions, en particulier pour les très petits montants. La publication de ces noms en 2009, à laquelle s'est référé Hans-Hermann Schild et dont la Cour a ordonné la suppression, figurait encore sur Internet au moment du symposium. Une preuve de plus, selon le juge, qu'Internet n'oublie rien.

Un cadre légal bien défini

Le Préposé à la protection des données du canton de Zurich, Bruno Baeriswyl, s'est exprimé pour sa part sur l'arrêt du Tribunal fédéral, l'été dernier, dans l'affaire de la FIFA, qui révèle clairement les tensions entre liberté d'information et protection des données. La pesée des intérêts se déroule dans un cadre légal bien défini, a-t-il expliqué. Il n'existe pour lui aucune transparence absolue, tout comme il n'y a pas de protection absolue de la sphère privée.

Concrètement, le Tribunal fédéral a confirmé en juillet le droit de journalistes de consulter une ordonnance de classement dans l'affaire de la FIFA et a ainsi rejeté le recours de deux fonctionnaires de cette instance qui s'étaient opposés à cette consultation. Dans son arrêt, le Tribunal fédéral conclut qu'il y a un intérêt important à la consultation de la décision de clôture de la procédure pénale. Il confirme ainsi le rôle d'observateurs des médias à l'égard de l'activité des autorités et l'intérêt du public à être informé sur les allégations de corruption au sein de l'association faitière du football mondial. Dans ce but, les noms des personnes concernées et les circonstances personnelles et financières prises en compte par les autorités doivent également être divulgués aux journalistes.



Contrôle des webcams du canton de Fribourg

La Préposée à la protection des données a effectué un contrôle sur les photos prises par des *webcams* touristiques placées sur le territoire du canton de Fribourg. Elle a constaté qu'un certain nombre de communes et de lieux faisait l'objet de prises régulières d'images sur lesquelles se retrouvaient des personnes identifiables, sans pour autant qu'elles aient donné leur consentement ou été informées de façon claire de l'existence et de la position des caméras. Ces photos se retrouvent aussi sur d'autres sites où elles sont enregistrées quelques heures ou quelques minutes, ce qui permet alors à des internautes experts de les enregistrer sans difficulté. Il existe dès lors des risques d'atteinte aux droits fondamentaux, notamment au droit à l'image. Les communes concernées ont été interpellées sur les mises en adéquation nécessaires.

Toutes les communes qui souhaiteraient mettre en place sur leur site un système de webcams, de manière directe ou indirecte, devront respecter la Loi du 25 novembre 1994 sur la protection des données (LPrD).

La médiation, une voie vers la résolution d'un conflit

—
Dans le cadre d'une demande d'accès, le droit d'accès fribourgeois prévoit une médiation en cas de désaccord. La demande en médiation peut être déposée par toute personne qui a présenté une demande d'accès à un document officiel et toute personne dont les données personnelles figurent dans un document faisant l'objet d'une telle demande. Mais comment une médiation se déroule-t-elle ?

La procédure de médiation a pour but de dégager rapidement, c'est-à-dire dans les 30 jours, un accord entre tous les intéressés. Elle implique très souvent des concessions de part et d'autre. La Préposée entend d'abord les deux parties et leur explique la procédure. Lors de la séance suivante, elle en assume le déroulement mais ne propose en principe pas ses propres solutions. Au contraire, ce sont les personnes directement concernées qui, avec son aide en qualité de médiatrice de toutes les parties, devraient trouver d'elles-mêmes une solution satisfaisante pour tous. La Préposée aide les parties à clarifier et à verbaliser leurs besoins et leurs intérêts. Elle veille au respect des règles de médiation convenues en début de séance et à l'applicabilité des éventuels accords. Si les parties parviennent à un accord, la procédure est considérée comme close. Celui-ci est consigné dans un accord de médiation et devient immédiatement exécutoire.

Une recommandation en l'absence d'accord

Si aucune solution satisfaisante pour toutes les parties n'est trouvée, la Préposée rédige une recommandation à l'attention de l'organe public compétent et de la ou des personne(s) concernée(s). Dans l'ensemble de la procédure, la Préposée a accès sans restrictions aux documents demandés afin de pouvoir déterminer si l'organe public a traité la demande conformément à la loi et de façon appropriée.

Lorsqu'une recommandation est émise, l'organe public doit rendre une décision. S'il se rallie à la recommandation, le renvoi à cette dernière peut faire office de motivation. Cette décision est susceptible de recours. La procédure de médiation ne peut pas être ignorée, c'est une étape impérative.

L'expérience montre que cette étape fait tout à fait sens. Sur les neuf procédures de médiation engagées à ce jour, quatre se sont soldées par un accord de médiation. Dans les cinq autres cas, l'organe public a suivi la recommandation de la Préposée à la transparence.

Informations aux organes publics



Recommandation sur l'accès à un rapport technique

Dans une recommandation, la Préposée à la transparence s'est prononcée pour que l'accès soit accordé à un rapport technique concernant le choix du site du futur centre sportif à Romont. La ville de Romont avait argué que le document en question était un outil de travail interne servant aux discussions du Conseil communal.

Dans sa recommandation, la Préposée à la transparence parvient cependant à la conclusion que dans le document en question, il ne se trouve pas de 'réflexions individuelles, échanges de vues et avis de nature politique ou stratégique' qui caractérisent, selon l'art. 29 al. 1 let. c LInf, les 'notes internes servant aux discussions des organes publics'. Au contraire, l'étude préliminaire est un rapport technique qui énumère des faits et qui procède à une analyse technique des sites sous la loupe. Il n'existe par ailleurs aucun intérêt privé ou public prépondérant qui aurait comme conséquence que l'accès au rapport devrait être restreint ou refusé.

Pour la Préposée à la transparence, le public a un intérêt légitime à avoir accès aux informations formant la base des décisions de son administration communale. Ceci d'autant plus quand il s'agit d'un projet de grande envergure comme c'est le cas de la présente situation. Le droit d'accès au rapport technique doit donc être reconnu. La commune a suivi la recommandation et a finalement accordé l'accès à ce rapport.

Droit d'accès à son dossier médical

L'art. 24 al. 3 de la LPrD (Loi du 25 novembre 1994 sur la protection des données, RSF 17.1) dispose que «lorsqu'il s'agit de données sur la santé, la communication peut être faite par un ou une médecin désigné-e par la personne concernée. Les dispositions de la loi du 16 novembre 1999 sur la santé sont réservées». Le principe du droit d'accès figure à l'art. 60 de la LSan (Loi sur la santé du 16 novembre 1999, RSF 821.0.1): «Le patient ou la patiente a le droit de consulter son dossier et de s'en faire expliquer la signification. Il ou elle peut s'en faire remettre gratuitement les pièces, en original ou en copie, ou les faire transmettre au ou à la professionnel-le de la santé de son choix». Ce même article prévoit en outre deux restrictions du droit d'accès,

à savoir que «ce droit ne s'étend pas aux notes rédigées par le ou la professionnel-le de la santé exclusivement pour son usage personnel, ni aux données concernant des tiers couvertes par le secret professionnel». En outre, «si le ou la professionnel-le de la santé a des raisons de craindre que la consultation du dossier ne puisse avoir de graves conséquences pour le patient ou la patiente, il ou elle peut demander que la consultation n'ait lieu qu'en sa présence ou celle d'un ou d'une autre professionnel-le désigné-e par le patient ou la patiente».

Communication d'une liste de nouveau-nés à une bibliothèque communale

Dans le cadre du projet «Né pour lire», une bibliothèque communale et scolaire a demandé au contrôle des habitants de lui communiquer la liste des nouveau-nés de la commune. La bibliothèque en question est un service communal intégré dans l'administration communale et occupant du personnel communal. L'art. 16 b LCH (Loi du 23 mai 1986 sur le contrôle des habitants, RSF 114.21.1) dispose que «le préposé peut, dans un cas d'espèce et sur demande, communiquer à une autorité ou à une administration publique les données dont elle a besoin pour l'accomplissement de sa tâche». Comme cette disposition ne porte que sur la communication dans un cas d'espèce, la communication d'une liste de nouveau-nés ne paraît pas admissible. L'art. 23 REC (Règlement 2 décembre 1986 sur l'état civil, RSF 211.2.11) mentionne en outre qu'«est interdite la communication à quiconque de listes de naissances, décès, mariages, d'adresses ou d'autres données du même genre». Le contrôle des habitants doit respecter cette disposition et ne peut dès lors pas communiquer la liste de naissances demandée. Pour que la bibliothèque puisse atteindre son objectif sans que la communication des données soit effectuée, nous lui avons conseillé de préparer, d'entente avec la commune, un courrier-type à l'intention des parents de nouveau-nés à transmettre par le biais de la commune qui collerait elle-même les étiquettes. La commune devrait alors également en informer la population, par exemple dans le Bulletin communal.

Communication électronique de données d'aide sociale

—

Les données d'aide sociale sont des données sensibles qui, tout comme les informations confidentielles, ne doivent en principe pas être transmises par courrier électronique. Il faut préférer l'envoi par poste ou la remise personnelle. Toutefois, si la voie électronique doit tout de même être utilisée, il est utile de se référer à la Feuille informative n° 4 de l'ATPrD pour que la communication reste confidentielle (http://www.fr.ch/atprd/files/pdf19/feuille_informative_n_4_communicationdonnees_courriel.pdf). Si la communication n'emprunte que le réseau cantonal (Intranet), les documents échangés doivent être chiffrés; le chiffrement (ou cryptage) d'un message le rend illisible à toute personne qui ne dispose pas du code secret (clé) qui a servi au chiffrement. A défaut de chiffrement, on peut admettre une protection par mot de passe. Par contre si la communication transite par les réseaux publics (Internet), non seulement les documents échangés doivent être chiffrés, mais il devrait y avoir aussi vérification de l'intégrité du message; la garantie doit être donnée que l'information n'a pas été dénaturée, accidentellement ou intentionnellement lors de son cheminement sur le réseau. Enfin, des mécanismes d'authentification devraient garantir que l'expéditeur est bien celui qu'il prétend être.

Utilisation des offres «cloud» dans le contexte scolaire

—

L'art 17 LPrD dispose que «*tout organe public qui traite des données personnelles est responsable de la protection des données*». Ce doit être d'autant plus le cas lorsqu'il s'agit de mineurs. L'utilisation d'un cloud peut être dangereuse, surtout en ce qui concerne les clouds publics, parce qu'il est presque impossible de maîtriser l'information lorsqu'elle est ouverte au public. Le respect des conditions légales, notamment relativement aux flux transfrontières (art. 12a LPrD), n'est pas non plus garanti. Nous considérons ainsi que les clouds publics devraient être au minimum interdits. Les clouds privés peuvent être admis s'ils restent en mains de l'Etat; ils risqueraient sinon d'être gérés de façon anarchique, souvent hors de Suisse. La gestion par l'Etat permet en effet le respect d'exigences pré-établies, notamment en matière de sécurité. L'impératif de la sécurité impose de prêter une attention particulière et régulière à la formation du corps enseignant et des élèves,

et d'interdire que des données sensibles soient mises à disposition par le cloud. Une réglementation claire, par ex. des Directives, devrait être établie notamment sur la mise à disposition de photos d'élèves par le biais du cloud. Cette réglementation devra prévoir des dispositions sur les contrôles de l'application des Directives ainsi que des moyens appropriés respectant les dispositions sur la protection des données.

Publication de photos des enfants des écoles

—

Une commune souhaitait publier sur son site internet les photos d'enfants des écoles prises lors d'un événement sportif. La publication de photos sur internet est un traitement de données personnelles au sens de l'art. 4 LPrD qui dispose que «*l'organe public n'est en droit de traiter des données personnelles que si une disposition légale le prévoit, ou, à défaut, si les dispositions réglant l'accomplissement de sa tâche l'impliquent*». En l'espèce, la publication ne semble ressortir ni de la loi ni de l'accomplissement des tâches de la commune. Les Directives du 1^{er} janvier 2006 de la Direction de l'instruction publique, de la culture et du sport concernant la publication de données personnelles par internet précisent au ch. 2.3 qu'il n'existe aucun intérêt public à connaître les données personnelles des élèves, mais que la publication d'une photo de classe peut être admise avec le consentement des élèves concernés ou du représentant légal pour les mineurs. Le consentement n'est en outre valable que s'il est éclairé, c'est-à-dire qu'il doit avoir été donné librement et en toute connaissance de cause. Il doit également être spécifique (avec détermination des objectifs exacts), explicite (impliquant une réponse active) et indubitable (il ne doit subsister aucun doute sur l'intention de la personne à donner son consentement). En l'espèce, le consentement doit être requis si l'enfant est reconnaissable. Dans ces cas, la durée maximale de la publication (2-3-4 semaines?) doit également être réglée. Sans consentement, la commune peut publier les photos à certaines conditions : elle ne peut publier que des photos contenant des vues générales suffisamment éloignées pour qu'aucun enfant ne puisse être reconnu; la résolution ne doit en outre pas permettre de «zoomer». Aucune information personnelle permettant l'identification indirecte de l'enfant ne doit figurer, tant sous la photo que sur le nom du fichier publié.

Arrêt de la CJUE du 16 octobre 2012 - Commission européenne contre la République d'Autriche

—
L'arrêt établit que la République d'Autriche n'a pas pris les dispositions nécessaires pour que la **Datenschutzkommission** (autorité de contrôle des données à caractère personnel, ci-après DSK) satisfasse l'exigence d'**indépendance** de l'art 28 § 1 de la Directive 95/46/CE¹. En effet, selon la législation autrichienne, le membre administrateur de la DSK est un fonctionnaire de la chancellerie fédérale, assujéti à une tutelle administrative (Dienstaufsicht). Même si le supérieur hiérarchique ne peut pas donner d'instructions, le simple pouvoir de contrôle dont il bénéficie suffit à entraver

l'indépendance de la DSK. De plus, le bureau de la DSK étant intégré à la chancellerie fédérale, le personnel de la DSK est composé de fonctionnaires de la chancellerie eux aussi soumis à la tutelle administrative, ce qui confirme l'important risque d'influence extérieure. Finalement, le chancelier fédéral dispose d'un droit d'information inconditionnel portant sur tous les aspects de la gestion de la DSK. L'arrêt confirme ainsi le principe selon lequel la seule indépendance fonctionnelle ne suffit pas à remplir l'exigence d'indépendance requise par la Directive; toute forme d'influence indirecte sur les décisions de l'Autorité doit également être exclue.

¹ Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.



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

-

Décembre 2012