



Newsletter

#02 / 2018

Chère lectrice, cher lecteur,

Les documents en lien avec la rémunération d'informateurs(trices) de la Police cantonale de l'Etat de Fribourg doivent être communiqués à un journaliste, sous une forme caviardée si nécessaire. Voilà ce que le Tribunal cantonal a ordonné à la Police cantonale dans son arrêt du 24 mai 2018.

Un journaliste de la RTS a demandé à obtenir certains renseignements sur la rémunération des informateurs privés auprès de la Police cantonale fribourgeoise. Il voulait notamment connaître les montants globaux et la réglementation traitant de la question des informateurs(trices) privé(e)s. La Police a refusé d'y donner l'accès en invoquant un intérêt public prépondérant. Dans sa recommandation et suite à l'échec de la médiation souhaitée par le journaliste, la Préposée à la transparence a retenu que le refus total d'accès était disproportionné au vu des arguments avancés par la Police cantonale. Elle a considéré qu'un caviardage des passages sensibles des documents demandés était suffisant pour préserver l'intérêt de la sécurité publique en jeu tout en permettant l'accès au contenu essentiel de ces documents. La Police cantonale n'a pas voulu suivre la recommandation et a maintenu son refus de donner accès à ces documents. Le journaliste a ensuite déposé un recours à la Direction de la sécurité et de la justice qui a confirmé cette décision, puis au Tribunal cantonal.

Dans son arrêt, le Tribunal cantonal a constaté que l'ordre et la sécurité publics figurent au rang des intérêts prépondérants retenus par la LInf (art. 26 al. 1 let. a LInf) qui peuvent justifier de restreindre, différer ou refuser l'accès aux documents officiels. Mais au vu du principe de la proportionnalité auquel l'organe public est tenu, il ne saurait refuser la transmission d'un document si une mesure moins incisive telle que le caviardage permet de sauvegarder l'intérêt public protégé. Dans le cas précis, le risque d'atteinte à la sécurité et à l'ordre publics n'était démontré ni dans son existence, ni dans son ampleur, tout au moins pas dans une mesure qui justifierait un refus intégral de la transmission des documents sollicités par le journaliste. Par conséquent, les documents demandés par le journaliste, à savoir les documents relatifs au budget annuel servant à la rémunération des informateurs pour les dix dernières années, de même que l'ordre de service y relatif de la Police cantonale, doivent lui être transmis, sous une forme caviardée si nécessaire.

Cet arrêt est important en matière de transparence et de droit d'accès aux documents officiels pour le canton de Fribourg. En effet, il rappelle que l'accès aux documents de l'administration est la règle, que les intérêts publics peuvent exceptionnellement justifier un refus, mais seulement si des mesures moins incisives telles que le caviardage ne suffisent pas.

Martine Stoffel
Préposée cantonale à la transparence



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
Guide pour les portails web de l'administration publique	2
Contrats informatiques	3
L'intelligence artificielle, une opportunité pour notre société ?	4
Arrêt du Tribunal cantonal du 13 septembre 2018	
Accès à ses données personnelles dans un PV d'audition d'une procédure pénale	5
Informations aux organes publics	6
Trois recommandations en matière de droit d'accès	6

Actualités

Guide pour les portails web de l'administration publique

Privatim, la conférence des préposé(e)s suisses à la protection des données, a publié un guide consacré aux exigences légales et techniques des portails web de l'administration publique permettant ainsi d'assurer la sécurité des données des citoyen(ne)s et de protéger leur vie privée. En effet, dans l'administration numérisée, les portails web font l'interface entre les citoyens et l'administration et offrent un service 24 heures sur 24. De ce fait, l'administration se doit de respecter la protection et la sécurité des données en ligne qui, selon Privatim, sont encore trop souvent négligées dans les projets de numérisation, soit à cause du manque de connaissances techniques nécessaires au projet, soit parce que les autorités responsables de la protection des données ne sont pas impliquées.

Ainsi, pour bénéficier durablement des opportunités offertes par la numérisation, une évaluation continue des risques et la mise en place de mesures de sécurité nécessaires s'imposent.

C'est dans le but de soutenir l'administration publique dans la planification et l'exploitation de portails web, que Privatim a publié la marche à suivre permettant de protéger les données des citoyen(ne)s et de mettre en œuvre des solutions numériques au service des citoyen(ne)s tout en respectant la législation en matière de protection des données.

Le guide définit les notions telles que vérification, identification, authentification et autorisation qui sont souvent, dans la pratique, confondues. Puis, il distingue les différents types de portails (portail de passage et portail de données de base) et mentionne les exigences liées à l'enregistrement d'un utilisateur, à son authentification et à la problématique de l'identificateur univoque. Enfin, des exemples concrets, les aspects juridiques ainsi que les mesures organisationnelles et techniques indispensables dans le cadre des portails web sont développés.

Voici le lien qui vous permet d'accéder directement au guide: http://www.privatim.ch/wp-content/uploads/2018/10/031018_privatim_Guide_portails_web.pdf.

Contrats informatiques

—

Lors du colloque du CEDIDAC, le 31 octobre 2018 à Lausanne, Juliette Ancelle (Id est) et Karim Ferdjani (IBM) ont traité des contrats informatiques à savoir ceux relatifs à la fourniture de produits ou services liés à la technologie informatique. De leur grande variété, ils en ont présenté 4 types: le contrat d'hébergement, XaaS – dit Cloud computing, d'outsourcing et de développement informatique. Ils soulèvent toutefois qu'il n'y a pas de définition uniforme, ni de cadre juridique unique. Le cadre légal dépend du contenu du contrat qu'il n'est pas toujours possible de définir en amont. Chaque contrat doit être négocié et contenir des clauses clés. En effet, le contrat général doit obligatoirement traiter de la description du périmètre des services en mettant un effort important à la rédaction, du niveau de services (Service Level Agreements; SLA), de la propriété intellectuelle, de la protection et la sécurité des données, de la responsabilité, des audits ainsi que de la résiliation. Dans la pratique, ils ont observé que ces informations font souvent défaut. Enfin, ils soulignent l'importance que ces contrats soient conclus par le service juridique et soient écrits de manière compréhensible pour toutes les parties.

Le point après 6 mois d'application du RGPD

Lors de ce même colloque du CEDIDAC, Sylvain Métille a, quant à lui, fait part de ses premiers constats de l'application du Règlement général sur la protection des données (ci-après: RGPD) depuis le 25 mai 2018.

Il relève que l'application du RGPD offre des opportunités commerciales. En effet, des formations de DPO (data protection officers) se sont multipliées. Toutefois, il note également des arnaques évidentes effectuées par des entreprises peu scrupuleuses et présentées comme «labellisées». Actuellement, il n'existe pas de certification officielle. En outre, il souligne que des erreurs dues à la panique ont lieu, telles que des demandes de consentement

contre-productives. Le RGPD a toutefois permis d'accroître la sensibilité des citoyens et des entreprises à la protection des données. En effet, il y a eu une augmentation de «plaintes» face au traitement de données, une baisse de l'utilisation de cookies, un effort de transparence chez les fournisseurs(euses) par exemple mais aussi des accords de sous-traitance et des clauses contractuelles facilement accessibles. Il relève que les informations relatives au traitement des données sont plus accessibles et plus intelligibles.

Sylvain Métille est toutefois d'avis qu'il y a encore du travail pour les autorités, en particulier en ce qui concerne l'adoption de lignes directrices pour l'application du RGPD, notamment lorsque le responsable de traitement ou le sous-traitant est établi en dehors de l'Europe, mais également pour les responsables du traitement. Cependant, il rappelle que la conformité n'est jamais acquise, de sorte qu'il faut continuer les efforts. L'entrée en application du RGPD a toutefois créé une forte prise de conscience des enjeux en matière de sphère privée.

L'intelligence artificielle, une opportunité pour notre société?

—
Le traitement des données franchit en permanence de nouvelles étapes. Alors que des interactions entre l'être humain et la machine étaient nécessaires jusqu'à présent, les machines devraient bientôt être autonomes. Qu'en est-il de la protection des données?

L'intelligence artificielle des ordinateurs représente un nouveau défi pour notre société. Si le traitement de grandes quantités de données repose sur des algorithmes mis au point par des humains, les machines sont désormais capables d'apprendre d'elles-mêmes pour prendre le relais de l'homme de manière autonome. Cette facette de l'intelligence artificielle figurait au programme de l'édition 2018 du «Symposium on Privacy and Security» organisé à Zurich le 6 septembre dernier.

La protection des données est-elle un obstacle à l'intelligence artificielle?

Dans son intervention, le professeur Buhmann de l'ETH Zurich a démontré que le big data constitue le moteur de l'intelligence artificielle, car seuls des algorithmes permettent de traiter ces énormes quantités de données. Par algorithme, on désigne des procédures de calcul décisionnelles consultant des valeurs sources et calculant des valeurs cibles. Des algorithmes capables d'apprendre créent désormais de la valeur ajoutée en explorant notre réalité dans toute sa complexité. Technologie basée sur l'imitation, l'intelligence artificielle n'est toutefois pas une méthode scientifique. Pour le professeur Buhmann, le recours personnalisé à l'intelligence artificielle dans la sphère privée constitue notamment un dilemme: un point de vue qu'il illustre en prenant l'exemple de la médecine personnalisée. Combiner la compression d'énormes quantités de données (p. ex ayant trait à des patients, des diagnostics, des pronostics et des traitements) à l'analyse de données via l'apprentissage de la machine permet d'acquérir de nouvelles connaissances et d'en tirer des bénéfices personnels pour les patients. Des progrès néanmoins impossibles à réaliser si ces données sont trop protégées et exclues du domaine de la recherche.

L'intelligence artificielle comme opportunité

Pour le professeur Koehler, l'intelligence artificielle constitue une véritable opportunité pour notre société: «L'intelligence artificielle attire l'attention sur certains éléments, tire des conclusions et agit de manière intelligente». Ses applications sont multiples: calcul du chemin le plus court, conduite autonome, applications linguistiques et traductions, traitement des images ou encore développement d'algorithmes. Les machines sont capables d'apprendre beaucoup plus rapidement que les humains, car l'espace de stockage fait défaut à ces derniers. L'intelligence artificielle fera disparaître des métiers peu valorisés et permettra d'élaborer des processus de production adaptés à la fois aux délais et à la demande.

Elle a également des applications dans le secteur public où elle est notamment déjà employée dans la gestion du trafic et l'attribution automatisée de permis de stationnement pour riverains. Sur le principe, le recours à l'intelligence artificielle en matière d'actes administratifs automatisés est accepté pour autant que sa logique soit claire et qu'aucune appréciation ne soit requise de sa part. Elle s'avère toutefois délicate à mettre en place dans les domaines dans lesquels la logique décisionnelle est complexe et opaque. De l'avis de Mike Weber, responsable suppléant du centre de compétences des systèmes de communication ouverts de l'institut Fraunhofer FOKUS, l'intelligence artificielle revêt également un potentiel considérable en matière d'amélioration de l'efficacité et de l'efficacé dans l'administration publique. Son recours est cependant tributaire de diverses réflexions socio-politiques, dont la question est de déterminer dans quelle mesure l'État doit être impliqué dans le développement de l'intelligence artificielle, comment faire face aux risques pour la sécurité ou encore comment assurer le bien commun. Enfin, il s'agit également de clarifier la question de l'accès aux données et de l'externalisation des tâches correspondantes.

Arrêt du Tribunal cantonal du 13 septembre 2018

Accès à ses données personnelles dans un PV d'audition d'une procédure pénale

A. souhaitait avoir accès aux déclarations faites par son frère B. au sujet d'un bien immobilier lui appartenant, dans le cadre d'une instruction pénale menée à l'encontre de B. Le Président du Tribunal d'arrondissement a rejeté la requête de A. Ce dernier a contesté cette décision auprès du Tribunal cantonal et en demande l'annulation.

Le Tribunal cantonal retient qu'après la clôture d'une procédure pénale, la consultation du dossier ne relève plus du Code de procédure pénale (CPP) mais de la législation cantonale, en particulier celle concernant la protection des données. En outre, l'accès aux procès-verbaux sollicités sur la base de la Loi sur l'information et l'accès aux documents (LInf) n'est de toute manière pas admis car les documents requis proviennent de séance non-publique, qui sont exclues du droit d'accès institué par cette loi. Le Tribunal cantonal rappelle que ce n'est pas parce qu'un document est soustrait au droit d'accès du public fondé sur la LInf qu'il ne peut pas être consulté en vertu du droit, pour une personne déterminée, d'accéder à ses propres données personnelles en vertu de dispositions sur la protection des données. A cet égard, il retient qu'un procès-verbal de séance contient des informations relatives aux personnes qui se sont exprimées durant une séance, mais également des données personnelles relatives aux personnes au sujet desquelles des affirmations ont été faites et qu'une expertise immobilière contient des informations relatives au bien expertisé, mais aussi indirectement au sujet du propriétaire du bien, qu'il soit nommément cité

dans l'expertise ou non. En l'espèce, le Tribunal cantonal a considéré, après une pesée des intérêts entre les intérêts de A. à avoir accès à ses données personnelles par le biais de la Loi sur la protection des données (LPrD) et ceux de B., prévenu dans la procédure pénale, que les extraits de PV sollicités étaient d'une portée très limitée, qu'ils ne permettaient pas d'établir de lien avec le reste de la procédure et que rien ne faisait obstacle au droit d'accès à ses propres données. Ainsi, A. a pu obtenir accès aux parties strictement limitées des procès-verbaux qui contiennent ses propres données.

L'arrêt peut être consulté par le biais de ce lien:

<http://publicationtc.fr.ch/?dec=40c99a90aa8948a382422af84157803c&index=TC>

L'arrêt 601 2018 27 du Tribunal cantonal du 24 mai 2018 mentionné dans l'éditorial en matière d'accès aux documents publics peut être consulté sous le lien suivant:

<http://publicationtc.fr.ch/?dec=4693ee87ebb5478e9745bd530f9a7f0e&index=TC>

Informations aux organes publics



Trois recommandations en matière de droit d'accès

Durant la deuxième moitié de l'année 2018, la Préposée cantonale à la transparence a rédigé trois recommandations. En outre, plusieurs médiations sont actuellement en cours.

Les deux premières recommandations traitent de deux oppositions de tiers concernés à l'**accès au rapport d'audit** mandaté par le conseil d'administration de l'Hôpital de Fribourg (HFR). Le but du rapport était d'analyser la gouvernance de l'HFR. Plusieurs personnes ont demandé l'accès au document suite à la publication d'un résumé du rapport d'audit et d'un communiqué de presse y relatif en février 2018. Le HFR s'est déterminé en faveur de l'accès au rapport sous une forme caviardée, mais deux tiers concernés s'y sont opposés en faisant valoir des intérêts privés prépondérants et ont déposé une demande de médiation. La Préposée cantonale à la transparence a recommandé d'accorder un accès partiel au rapport. Elle a considéré que son contenu peut porter atteinte à la sphère privée des personnes concernées et a recommandé de caviarder quelques passages supplémentaires par rapport à la version proposée par l'HFR. Elle a été d'avis que l'intérêt du public à avoir accès au rapport l'emporte sur l'intérêt privé des deux personnes de maintenir le rapport secret. L'HFR a suivi dans sa décision la recommandation de la Préposée. Un des tiers concernés a déposé un recours au Tribunal cantonal.

La troisième recommandation se penche sur une demande d'**accès à une décision d'une préfecture** concernant l'entretien des canalisations d'eaux usées dans un secteur d'une commune du canton. Cette décision tranchait des recours déposés par différents propriétaires du secteur contre une décision de la commune. Après consultation des tiers concernés et malgré l'opposition d'un de ceux-ci, la préfecture s'est déterminée en faveur de l'accès intégral à la décision. Le tiers qui s'y est opposé a alors demandé une médiation auprès de la Préposée cantonale à la transparence en faisant valoir des intérêts privés prépondérants. La Préposée a considéré que les éléments invoqués ne concernaient pas la sphère privée protégée de la personne et ne constituaient dès lors pas des intérêts privés prépondérants pour s'opposer à une demande d'accès. Elle a recommandé d'accorder l'accès à la décision; dans sa décision, la préfecture a suivi cette recommandation.



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

-

Janvier 2019