Newsletter
#02 / 2014

Chère lectrice, cher lecteur,

La protection des données et les archives ont bien des points communs, comme l'a récemment révélé une journée archivistique. C'est également vrai pour les archives judiciaires. Une gestion sérieuse des données y est tout aussi essentielle. Tandis que les droits de la personnalité constituent un bien à protéger au cœur de la protection des données, les archives font office de mémoire de la société. Pour la protection des données, il découle du principe de proportionnalité que les données personnelles doivent être détruites ou rendues anonymes si elles ne s'avèrent plus nécessaires, sous réserve néanmoins des dispositions relatives à l'archivage. Celui-ci porte quant à lui sur l'aspect historique. Il y est question de la protection des données et des matériaux au regard de la conservation des documents de l'époque.
Le but de la collecte des données personnelles change si elles sont archivées: alors que la protection des données part de l'idée d'un traitement conforme à la finalité et la destruction des données lorsqu'elles ne sont plus utilisées, l'archivage se concentre sur la conservation et le stockage afin de documenter l'histoire contemporaine. La gestion des données personnelles est consciencieuse et minutieuse lorsque les données et les informations archivées ne sont pas immédiatement accessibles au public, mais seulement après l'expiration d'un délai de protection. Il est indispensable de prévoir des délais appropriés pour les documents qui comportent des données personnelles, voire sensibles, à l'instar des documents de nature policière et des dossiers judiciaires. Sur ce point, la législation du canton de Fribourg témoigne d'une gestion efficace des données personnelles et démontre que les droits de la personnalité sont pris au sérieux. Fort heureusement, l'avant-projet de Loi sur l'archivage et les Archives de l'Etat prévoit des délais de protection étendus. Voilà qui est essentiel aujourd'hui, avec les innombrables sources d'information, moyens de publication, médias sociaux et en particulier Internet, qui ne connaît pas de «droit à l'oubli». Les nouveaux médias permettent de suivre «l'histoire» d'une personne des années plus tard. Ainsi, une divulgation prématurée des archives judiciaires ne respecte pas l'intangibilité des droits de la personnalité. Au contraire, l'archivage sans délais de protection suffisants peut, en relation avec les nouveaux médias, perpétuer les atteintes à la personnalité. Dans ce contexte, et notamment à l'aune du droit à l'oubli, l'avant-projet et ses délais de protection exemplaires montrent la voie à suivre.

Alice Reichmuth Pfammatter
Préposée cantonale 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

EC 902

Sommaire

Actualités

Septième Journée suisse du droit à la protection des données

La journée suisse du droit de la protection des données, à l'Université de Fribourg, a cette année mis l'accent sur «la mise en œuvre des droits des particuliers dans le domaine de la protection des données». En effet, l'évolution des technologies étant toujours plus rapide, de nouveaux instruments de protection tels que le privacy by design, le droit à l'oubli numérique ou encore les règles d'entreprise contraignantes prennent leur essor.

Les défis actuels posés par les avancées techniques et les changements comportementaux poussent les différents organes compétents à réagir. En mars 2014, le Parlement européen a adopté quelques changements au projet de règlement général sur la protection des données, dont le renforcement des droits des personnes concernées ainsi que la mise en place de nouveaux instruments de protection tel que le privacy by design (protection intégrée de la vie privée, PIVP).

Transfert de données

De nouveaux instruments tels que les BCR (Binding corporate rules ou règles d'entreprise contraignantes) sont aujourd'hui à prendre en compte. Il s'agit d'outils de conformité permettant d'encadrer les transferts de données au sein de groupes internationaux, a expliqué M^{me} Myriam Gufflet, responsable du Pôle BCR, direction de la Conformité à la Commission nationale française de l'informatique et des libertés (CNIL). Bien que la Suisse ne soit pas encore directement concernée, avec des multinationales telles que Nestlé, ADM, Adecco, etc. une petite introduction semble de circonstance.

Les BCR visent les transferts de données hors de l'Espace économique européen (EEE). En principe, les transferts de données sont interdits (art. 25 directive 95/46/CE), sauf en cas de dérogation. Ainsi le pays ou l'entreprise qui souhaiterait faire usage de cette possibilité (transferts de données hors EEE) doit offrir un niveau de protection adéquat, voire répondre à des exigences telles que la mise en place de transferts encadrés par des Clauses contractuelles types. L'appréciation du niveau suffisant de protection est faite

par la Communauté européenne (CE). M^me^ Myriam Gufflet a expliqué dans son exposé que les BCR est un code de conduite définissant la politique globale d'une entreprise en matière de transferts de données personnelles hors EEE. Dès lors, la mise en place des BCR au sein de l'entreprise facilite la gestion ainsi que le transfert de données au sein d'une multinationale.

Reconnaissance des droits

La citation de la journée: «je ne sais qu'une chose, c'est que je ne sais rien», illustre très bien la situation présente. M^e^ Olivier Gnehm, avocat à Zurich, a commencé sa présentation sur cette citation de Platon et poursuit ainsi «si et comment mes données sont traitées». Comme l'a relevé Jean-Philippe Walter, Préposé fédéral suppléant à la protection des données et à la transparence, les particuliers ont non seulement une méconnaissance de leurs droits, mais les responsables de traitement ont également une connaissance insuffisante de la Loi fédérale sur la protection des données (LPD; RS 235.1) et des outils de protection mis en place. Cela se traduit principalement par un usage restreint des possibilités offertes par les offices fédéraux. M^me^ Monique Cossali Sauvain, Cheffe de l'unité Projets et Méthodes législatives auprès de l'Office fédéral de la justice (OFJ), a affirmé que les réflexions de refonte de la loi (LPD) vont notamment dans le sens d'une meilleure sensibilisation des personnes concernées, mais vise également une protection optimale en amont, afin de détecter les éventuels problèmes dès la phase de conception de nouvelles technologies.

Identité numérique

«Notre identité se compose d'un certain nombre de facettes qui s'expriment de manière différente, en fonction du contexte social», a déclaré Stéphane Koch, Vice-Président de High-Tech Bridge SA. En ces temps de modernité, contrôler son «identité numérique» est parfois un «casse-tête», et bien que la plupart des réseaux sociaux ou autres plateformes (tels que Facebook, Twitter, LinkedIn, Instagram, skype, etc.) offrent différents moyens de sécuriser ou même d'effacer nos données, cela n'est pas toujours suffisant. Dès lors, il devient primordial d'équilibrer le «droit à l'oubli numérique», la nécessité d'exister numériquement, la liberté d'expression et le droit d'être informé. Et si à l'heure actuelle, il est admis que l'écoulement du temps donne en principe aux personnes concernées le droit de s'opposer à ce que soient à nouveau révélés des faits appartenant au passé (droit à l'oubli), une pondération des intérêts en présence est néanmoins essentielle. Les médias, par exemple, ne se privent pas d'exploiter la moindre information; notre moyen de défense, le droit à l'oubli.

Une première victoire a été la décision de la Cour de justice de l'Union européenne qui pose que toute personne a le droit de demander que les moteurs de recherche suppriment, dans les résultats de recherche, les informations personnelles la concernant. La réaction de Google, avec la mise en place d'un formulaire «droit à l'oubli», dont 12'000 demandes ont été enregistrées en 24 heures, attire notre attention. Stéphane Koch s'est déclaré intéressé à voir comment Google va s'y prendre pour gérer ce nouvel instrument.

Diversité de questions

Dernier intervenant de la journée, le Professeur Alexandre Flückiger, Vice-Doyen et Professeur à l'Université de Genève, a présenté un bref aperçu des derniers arrêts du TF en relation avec la protection des données. Ce faisant, il a démontré la diversité des questions que soulève le sujet (de l'indépendance d'une autorité de contrôle en matière de données, en passant par le contrôle d'identité lors de manifestations sportives, la rectification de procès-verbaux ou encore la question des dossiers hospitaliers, etc.). Toutes ces décisions témoignent de l'importance et du rôle non négligeable de la protection des données dans notre société.

Sous la direction de la Professeure Astrid Epiney de l'Université de Fribourg, cette septième journée s'est achevée sur un constat clair: la Suisse ne peut agir sans tenir compte de ses voisins. Et en raison des accords Schengen et Dublin, la Suisse se doit d'être en conformité avec le droit européen; modèle intéressant, voire référence possible, pour une révision efficace et pragmatique. Partant, la nécessité de prendre des mesures concernant les mécanismes d'exécution, le besoin de mettre en place des instruments de protection adéquat ainsi que le besoin de réforme et d'adaptation de nos lois à la réalité sociale sont les perspectives d'avenir du droit de la protection des données.

Symposium on Privacy and Security

—

Fin août s'est tenu à Zurich le 19e Symposium on Privacy and Security, journée consacrée à la protection des données et à la sécurité informatique, avec pour titre «Datenschutz in der Datenflut? «Big Data Analytics» – Möglichkeiten und Herausforderungen. Technische, rechtliche und gesellschaftliche Konzepte auf dem Prüfstand».

En cette ère numérique, la sécurité apparaît toujours plus fragile, les technologies d'information semblent être des facteurs de risques et les valeurs fondamentales de notre société dont la liberté personnelle et la sécurité sont en jeu. Alors qu'aucun concept global de protection n'est à ce jour envisagé, ni véritable réforme, sensibiliser la population aux différentes formes d'autoprotection (utilisation judicieuse d'Internet, connaissance et compréhension des moyens informatiques, etc.) semble être le moyen le plus rapide, en l'absence de sécurité juridique.

Big Data

Alors que le volume disponible de données ne cesse d'augmenter, l'apport de ces dernières pour les secteurs économiques favorise un rapprochement entre «Big Data» et «Big Business». En d'autres termes, ces données générées et développées par notre société d'information sont de nouvelles valeurs économiques sur le marché (ex. Amazon, Zalando, Facebook, Whatsapp,...). Le Professeur Thomas Hofmann, Professeur de «Data Analytics» au Département Informatique à l'ETH Zürich, a principalement présenté ce magma d'informations sous trois axes: volume, «velocity» et variété. Le «volume» signifie qu'en terme quantitatif, la multiplication de données et bases de données est importante non seulement en raison du World Wide Web et des «smart devices» tels que les smartphones et tablettes, mais également en raison de l'usage que l'Homme en fait. Le Professeur a utilisé l'expression «toutes les informations sont sur Google, tout le monde est sur Facebook et tous les produits sont sur Amazon» pour appuyer son propos. L'étendue quantitative de ces informations est amplifiée par leur mode de création. Aujourd'hui cette masse s'auto-génère par un système d'autocréation automatique (sensoring, tracking, environnement, self-posting, etc.). Cette auto-productivité est ce que le Professeur nomme «velocity». Ajoutons que cette «velocity» est caractérisée par sa diversité. Ainsi, cette densité d'informations auto-générée varie dans ses sources (web surfing, ticket de caisse, réseaux sociaux, géolocalisation, etc.), mais également dans le type même de données (informations personnelles, relevés bancaires, données sociales, etc.). Dès lors, «Big Data» est non seulement source de changements dans différentes branches industrielles présentant un potentiel pour notre économie (média, publicité, e-commerce, santé, éducation, etc.), mais par son absence de limite, ou frontière, il offre également une perte de contrôle et présente un risque pour la protection des données notamment par des abus politiques et gouvernementaux – souvenons-nous du cas d'Edward Snowden.

IT – Protection adéquate?

Aujourd'hui, avec l'essor des nouvelles technologies et moyens de communications, le citoyen lambda a plus que besoin d'une protection adéquate de ses données. Lors de cette journée, le Professeur Norbert Pohlmann, de l'institut pour l'Internet-Sicherheit – if(is) Westfälischen Hochschule, a présenté les quatre grands défis que soulève la sécurité informatique: la sensibilisation face aux données à protéger, la prévention des attaques, la reconnaissance d'attaques et la réaction (contre-attaques) face à celles-ci. Première surprise, seulement 5% des données disponibles seraient véritablement dignes de protection.
La question qui fâche demeure toutefois: comment identifier ces données et mettre en place un système de protection convenable? En terme de prévention et sensibilisation, le principe directeur est l'économie de données, c'est-à-dire générer le moins de données possible, mais autant que nécessaire. De plus, la réactivité des utilisateurs par la mise en place de systèmes de protection (système de sécurité codé ou brouillé, procédure d'authentification, système informatique digne de protection, antivirus, anti-spam, nettoyage fréquent des caches et cookies, etc.) minimise, voire supprime, tout risque (virus, logiciels malveillants, spam, etc.). L'expérience montre cependant que les nouvelles technologies de sécurité n'offrent ni solution ni programme suffisamment efficace et digne de confiance. Ainsi, la possibilité offerte par certains programmes de reconnaître toutes attaques malveillantes ou anomalies dans le système est certes utile, mais possède néanmoins des limites.
En conclusion, il est vrai que la sécurité informatique présente de grandes lacunes, que le citoyen est constamment exposé à des menaces et que nos valeurs fondamentales sont quelque peu revisitées. Cependant, le progrès technique est une source de facilité et d'ouverture pour la société actuelle et, bien que le volume de données ne soit

pas moindre et que l'accès à l'information soit toujours plus aisé, la sensibilisation, la prévention et l'information des utilisateurs doivent être renforcées. Ce colloque s'est voulu analytique et préventif tout en présentant une vue d'ensemble de la situation.

IT – Cas du «Phishing»

La sécurité informatique est chaque jour mise à rude épreuve (hacking, vol d'identité virtuelle, etc.). Un problème nouvellement rencontré par les utilisateurs d'Internet est le «Phishing ou hameçonnage» qui se définit comme le vol d'informations sensibles telles que les données d'identification des internautes. Le terme anglais phishing est un mot-valise composé de «password» et de «fishing» et signifie donc littéralement «pêche aux mots de passe». En un mot comment cela fonctionne: il s'agit de la collecte via Internet ou e-mail de données sensibles, de mots de passe (login), de données de carte bancaire, de données d'accès à votre compte d'e-banking, d'informations concernant vos comptes sur des boutiques en ligne, voire de données de connexion à des comptes e-mail et réseaux sociaux. Des personnes se faisant passer pour un expéditeur que vous connaissez vous demandent de leur renvoyer vos informations de compte par e-mail ou via un lien contenu dans un e-mail, ou encore vous envoient des e-mails publicitaires avec un hyperlien vers un site où vous pourriez soi-disant trouver des offres promotionnelles. Malheureusement derrière ces liens se dissimulent des sites Internet dont l'adresse et le contenu ressemblent à s'y méprendre à ceux de véritables prestataires de services en ligne (e-banking, vente par Internet, etc.). Ces e-mails d'hameçonnage peuvent également contenir des fichiers-joints et d'un simple clic sur ce dernier, vous installez un virus qui enregistrera tout ce que vous saisissez sur votre clavier. Les hackers s'en servent par la suite à des fins abusives. La recommandation est de ne jamais utiliser un ordinateur à des fins non seulement privées, mais également professionnelles. Il est fortement conseillé de ne pas utiliser l'ordinateur sur lequel vous surfez librement sur le net pour faire vos versements et paiements e-banking. De plus, les certificats de sécurité tel que le «https» sont une garantie de sûreté auquel tout utilisateur peut légitimement se fier, remarquons qu'un petit «cadenas» apparaît souvent au bas de telles pages.

Transparence – Idéologie d'un concept clé

Le monde actuel est une grande masse d'informations diverses et accessibles. Dans cette perspective, le Professeur Mandred Schneider de Ruhr-Universität-Bochum a soulevé, lors du 19e Symposium on Privacy and Security, la portée du principe de la transparence comme concept clé de l'économie et de notre quotidien. Cette approche semble prendre de plus en plus de poids. En effet, la quête de la transparence que ce soit d'un point de vue politique, économique et social ne cesse d'occuper les esprits. En avance sur son temps, Jean-Paul Sartre a prôné la transparence: «Je pense que la transparence doit en tout temps se substituer au secret», et a anticipé la tendance de ces dernières années dans bons nombres de pays (levée du secret bancaire dans le domaine fiscal ou encore le cas «Snowden»). Le président américain Barack Obama, lors de son discours d'investiture en 2009, a reconnu l'importance d'une politique transparente pour un système efficace.

En outre, la «transparence» de notre société est caractérisée par son architecture urbaine. Paul Scheerbart, dans «L'architecture de verre», présente de nouveaux procédés architecturaux (structures portantes métalliques, murs-rideaux de verre, etc.) qui auraient dû à ses yeux pouvoir transformer la vie des hommes: «le verre n'est pas pour rien un matériau si dur et lisse, sur lequel rien ne s'accroche. [...] Le verre en général est l'ennemi du secret». Ainsi, l'architecture transforme nos valeurs. Bien qu'oublié, le projet de Scheerbart (l'ordre du sensible) semble s'être réalisé dans les grandes métropoles, voire quelques plus petites villes. En se promenant dans ces espaces urbains, il est aujourd'hui habituel d'apercevoir de grands buildings aux façades réfléchissantes, ensemble de formes et d'images où nous évoluons. Et comme dans l'œuvre d'André Breton «Nadja», l'individu semble vivre dans une serre où tous les faits et gestes sont épiés et rendus visibles grâce aux nouvelles technologies.

Drones, les règles se durcissent

—

Depuis les récents évènements de Zurich, dont celui de juin dernier où un drone s'est excessivement rapproché du public lors du concert d'un célèbre groupe anglais, la Confédération a décidé de préciser la réglementation en vigueur.

En raison du nombre toujours plus important de drones, l'Office fédéral de l'aviation (OFAC) s'est vu dans l'obligation de réagir. L'office a ainsi jugé important d'adapter les dispositions légales. La mise à jour de l'Ordonnance du DETEC sur les aéronefs de catégories spéciales (OACS; RS 748.941) est ainsi entrée en vigueur le 1er août 2014. Ces modifications soumettent à tout déplacement de drones, dans un rayon de moins de 100 m, l'obligation pour le pilote d'obtenir une autorisation de l'OFAC.

Les points suivants ont également été ajoutés:

- pour les drones allant de 0.5 kg à 30 kg, l'autorisation de l'OFAC n'est pas nécessaire; la condition est cependant que le pilote garde en tout temps un contact visuel avec le drone;
- pour les drones dont le poids excède 30 kg, les vols sans contact visuel à moins de 100 m de distance d'un attroupement de foule, notamment lors de «public viewing» et de tout événement public rassemblant plusieurs dizaines de personnes, sont soumis à autorisation de l'OFAC.

Lien vers l'ordonnance du DETEC
http://www.admin.ch/opc/fr/classified-compilation/19940351/index.html

Une transparence totale en cas d'utilisation de fonds publics

—

A l'échelle fédérale, il a souvent été question l'année dernière de l'utilisation de fonds publics au regard du principe de la transparence. Dans plusieurs recommandations, le Préposé fédéral à la protection des données et à la transparence (PFPDT) s'est prononcé pour une transparence totale.

C'est la seule façon de faire face à une utilisation détournée des fonds publics, a expliqué le Préposé fédéral à la protection des données et à la transparence, Hanspeter Thür, à l'occasion de la conférence de presse annuelle. Il observe donc avec inquiétude la volonté de plusieurs offices et services de s'affranchir de la Loi sur la transparence (LTrans). L'évaluation de cette dernière, initiée pour cette raison, ne doit pas mener à l'apparition de nouvelles zones grises non soumises à surveillance, en particulier dans le domaine de la surveillance où la transparence est primordiale.

Ces dernières années, l'aspiration constante à la transparence a permis de révéler quelques cas de corruption et d'abus à l'échelle fédérale, a rappelé Hanspeter Thür. L'affaire de corruption au Secrétariat d'Etat à l'économie notamment a éclaté au grand jour grâce à la LTrans. Une recommandation du PFPDT a en outre divulgué les dessous du financement privé de chaires de l'EPF, avec pour corollaire des débats publics enflammés.

Plusieurs recommandations ont également visé l'octroi de subventions et de fonds d'innovation, la publication de contrats entre l'administration fédérale et des experts ou des entreprises qu'elle a mandatés de même que les liens d'intérêt du personnel de la Confédération. «Dans tous les cas, il est question de l'utilisation des fonds publics. Nous sommes clairement d'avis qu'il est nécessaire d'instaurer une transparence totale en l'espèce», conclut le Préposé.

Informations aux organes publics

Demande en médiation pour des documents de la CEP Poya

La Préposée à la transparence a reçu une demande en médiation de la part d'une journaliste qui avait exigé auprès de la Commission d'enquête parlementaire (CEP), l'accès à sept procès-verbaux d'entrevues de politiciens et personnes impliquées dans le projet qu'avait réalisées la CEP, mais qui n'avaient pas été publiés dans le cadre du rapport final. La CEP a refusé l'accès aux documents au motif qu'il s'agit de procès-verbaux de séances non publiques qui, en vertu de la LInf, ne sont pas accessibles.

La Préposée à la transparence a pris connaissance de ces documents, parvenant elle aussi à la conclusion qu'il s'agissait de procès-verbaux de séances non publiques. Elle a néanmoins signalé au Secrétariat du Grand Conseil qu'il n'y avait pas de garantie d'accès pour les cas mentionnés à l'art. 29 LInf, mais que l'organe public pouvait l'accorder de son plein gré dans la mesure où toutes les parties impliquées y consentaient. L'organe public leur a alors demandé leur accord et les documents ont été remis à la journaliste.

Mise à jour du guide pratique sur le droit d'accès à l'attention des organes publics

Le guide pratique sur le droit d'accès à l'attention des organes publics a fait peau neuve suite à l'entrée en vigueur de la Convention d'Aarhus en Suisse. Il est disponible sur notre site Internet. Jetez-y un œil!
(http://www.fr.ch/atprd/fr/pub/publications/transparence/guide_pratique.htm)

Base de données des experts et des publications scientifiques sur le principe de la transparence

La plate-forme en ligne www.loitransparence.ch propose désormais une base de données des experts et des publications scientifiques sur le principe de la transparence. Celle-ci réunit plus de 120 études et articles scientifiques traitant du principe de la transparence dans l'administration fédérale, cantonale et dans celle d'autres pays. Ces contributions proviennent d'une cinquantaine d'experts dont on peut consulter les ouvrages et obtenir les coordonnées.

Installation d'une webcam

Une commune a saisi notre Autorité afin de connaître la procédure à suivre lors de l'installation d'une webcam, par un particulier, portant en tout ou en partie sur des lieux publics. En vertu de l'art. 1 al. 3 de la Loi du 7 décembre 2010 sur la vidéosurveillance (LVid), on entend par vidéosurveillance toute observation de personnes ou de biens effectuée au moyen de dispositifs techniques dans un **but de surveillance.** Le message du Conseil d'Etat du 6 juillet 2010 accompagnant le projet de Loi sur la vidéosurveillance mentionne expressément que la loi ne vise que les installations permettant l'observation des personnes à des fins de surveillance («vidéosurveillance dissuasive») à l'exclusion des dispositifs visant **un but purement récréatif,** par exemple les webcams dont l'installation reste libre pour autant qu'elle respecte les règles ordinaires de la protection des données. Partant, il ressort de la LVid et du message que le but de l'installation est déterminant pour savoir si la LVid s'applique à l'installation d'une webcam. Ainsi, si le but est récréatif, l'installation ne tombe pas sous le coup de la LVid, mais doit respecter la législation sur la protection des données. Par contre, si la webcam est installée dans un but de surveillance, elle est régie par la LVid et doit faire l'objet d'une autorisation octroyée par le Préfet de la commune sur le territoire de laquelle l'installation est envisagée.

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 2014