Newsletter
#01 / 2017

Chère lectrice, cher lecteur,
«L'ère numérique et la protection de la sphère privée»: le thème choisi pour les 10e Journées suisses du droit de la protection des données s'attaque à ce que Gilles Babinet, entrepreneur et représentant de la France auprès de la Commission européenne pour les enjeux de l'économie numérique, dans son article «L'ère numérique, un nouvel âge pour l'humanité», déclame comme une rupture de paradigme majeure pour l'ensemble de l'humanité.
En effet, la distribution très massive du savoir et des techniques de santé, l'émergence de la robotique, le changement de dimension des Etats, sont quelques-unes des notions fondamentales qui seront appelées à changer le cours de l'humanité.
A cet égard, il est symptomatique de constater que l'ère numérique permet de rendre l'information plus disponible qu'elle ne l'a jamais été et cela pour un coût insignifiant. A titre d'exemple, Gilles Babinet note, je cite: «En réalité, l'information à laquelle peut accéder un chercheur en physique quantique immergé dans le monde scientifique est pour ainsi dire semblable à celle à laquelle peut accéder un paysan au fond du Guatemala; ce qui diffère, c'est la capacité de ce dernier à l'utiliser; mais en soi, l'information est là.» Alexandre Demidoff, journaliste culturel, l'a résumé en un titre éloquent: «A l'ère numérique, l'érudit sait partager son savoir.»
Les questions qu'il y a lieu de se poser sont notamment les suivantes: quelle est l'échelle des changements induits par le numérique auxquels nous pouvons nous attendre et dans quelle mesure la protection de la sphère privée risque-t-elle d'être affectée? Les conférences de grande qualité données le 2 juin dernier à l'Université de Fribourg ont apporté tout autant d'éléments de réflexion que des débuts de solution!
A mon humble avis, il est indéniable que la révolution liée à l'ère numérique sera plus rapide qu'aucune autre et qu'il importera d'être des plus vigilants.
L'attention qu'il conviendra d'apporter à ce phénomène est d'autant plus grande qu'il porte sur des domaines infinis, tels l'éducation, la santé, l'économie et même l'Etat. En effet, tout ou presque peut être numérisé.
J'en veux entre autres pour preuve: l'éducation numérisée qui tend à se démocratiser par l'intermédiaire des MOOCs, soit massive open online course ou cours en ligne ouvert et massif; le séquençage génétique où l'ADN apparaît comme un paramètre essentiel; l'automatisation ou la robotique qui tend à envahir de plus en plus d'entreprise ou encore les systèmes digitaux qui pourraient s'initier dans la sécurité intérieure ou extérieure, l'émission de monnaie, la planification urbaine etc…
Face à ce défi, il me semble indispensable que la sphère privée soit préservée. La législation devra alors non seulement être suffisamment claire, mais aussi être rapidement adaptable afin d'éviter d'être dépassée.
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

L'ère numérique et la protection de la sphère privée

Début juin à Fribourg, la dixième Journée suisse du droit de la protection des données a abordé le thème de l'ère numérique et de la protection de la sphère privée sous différents angles. Il a été question des défis actuels à l'ère numérique aussi bien en droit de la protection des données qu'en droit des contrats.

«Si le choix du thème est banal, ce dernier ne l'est pas du tout», a souligné le Préposé fédéral à la protection des données et à la transparence, Adrian Lobsiger, en guise de préambule. Selon lui, la numérisation est plutôt un style de vie qui s'empare de nous. C'est un modèle économique auquel tout le monde veut participer – la Suisse aussi, bien entendu. Il n'y a donc pas d'autre choix que d'empoigner le sujet pour l'influencer, même si les développements nous ont surpris.

«Nous devons agir de toute urgence»

Dirk Helbling, Professeur à l'EPF de Zurich, a fait remarquer que nous sommes arrivés à une époque où l'homme et l'humain n'ont plus d'importance, seules les données comptent encore. D'après lui, les données recueillies peuvent par exemple servir à influencer les électeurs. Il a cité le cas d'une entreprise qui, par une nouvelle méthode, analyse minutieusement les gens à l'aune de leurs profils Facebook et contribue ainsi à la victoire des politiciens.

Avec dix «likes» sur Facebook, ce modèle sera capable de mieux évaluer une personne qu'un collègue de travail moyen. 70 «likes» suffiront pour dépasser la connaissance d'un ami et 150 celle des parents. «Avec 300 «likes», la machine pourra mieux prédire le comportement d'une personne que son propre partenaire», a expliqué Dirk Helbling.

L'humanité doit agir de toute urgence. D'une part, les législations sur la protection des données présentent d'immenses lacunes qu'il faut combler. D'autre part, il est nécessaire de répartir le contrôle de notre planète d'une manière participative, faute de quoi il risque de se perdre.

Réflexion sur les institutions étatiques

Dans un domaine où les changements s'opèrent à une vitesse accélérée, il est important de la part des juristes, qu'ils agissent au niveau institutionnel. Selon Bertil Cottier, Professeur à l'Université de la Suisse italienne, le principe de légalité, en vertu duquel le droit est la base et la limite de l'Etat, ne peut faire face à l'imprévisibilité et à l'incertitude que suscite le monde numérique. Face à lui,

le législateur a tendance à être dépassé, car le processus législatif met du temps à se mettre en marche. Ceci est en partie due à des procédures inadaptées et trop longues. Il règne alors une grande insécurité juridique.

Bertil Cottier a mis également en avant le fait que les instruments participatifs, qui laissent aux entreprises privées une certaine marge de manœuvre, sont utilisés à leur avantage afin de faire en sorte que ces dernières ne soient pas victimes de mesures restrictives de la part de l'Etat. Ce phénomène a mené les juristes à se pencher sur de nouveaux mécanismes législatifs. Les recommandations de bonnes pratiques, comme décrites dans l'avant-projet de la Loi sur la protection des données et pouvant être rédigées ou approuvées par le ou la Préposé/é fédéral/e à la protection des données et à la transparence, seraient une solution. On regrette cependant que celles-ci ne soient pas contraignantes. L'intervenant a proposé alors l'établissement d'une commission indépendante responsable de la protection des données pouvant rendre des recommandations contraignantes.

Dans la même lignée, Jean-Philippe Walter, Préposé fédéral suppléant à la protection des données et à la transparence, a suggéré que les lois soient moins détaillées et qu'il y ait une plus grande liberté d'action de la part des Préposés afin que ceux-ci puissent s'adapter à l'évolution ayant lieu chaque jour. Il a préconisé également l'utilisation de la technologie car celle-ci n'a pas que des aspects négatifs. «Sans nouveauté, les business modèles vont nous devancer». Du côté de Thomas Probst, Professeur à l'Université de Fribourg, les dispositions du droit des obligations contiennent toutes les normes nécessaires afin de relever les défis de la digitalisation. Selon lui, le problème ne se situe pas tant dans le contenu de la loi mais plutôt dans sa juste application, notamment dans la garantie des principes fondamentaux, tel le consentement éclairé.

Autant les termes abordés dans les exposés et ateliers étaient vastes, autant les référents et les participants à la journée étaient unanimes à le dire: les défis de la digitalisation sont multiples et posent toujours des questions plus complexes. Il n'est cependant pas encore trop tard pour la mise en place de mesures concrètes et dynamiques.

La surveillance de la correspondance par poste et télécommunication

—

La nouvelle Loi sur la surveillance de la correspondance par poste et télécommunication a pour but d'assurer un équilibre entre la surveillance et la sphère privée. Elle n'est applicable qu'à des conditions restrictives et dans le cadre de la procédure pénale, d'entraide judiciaire, ainsi que de la recherche de personnes disparues ou de personnes condamnées. La loi prévoit deux manières différentes de collecter les données: la surveillance en temps réel qui consiste à dévier le contenu d'une communication ainsi que la surveillance rétroactive. L'IMSI-catcher qui intercepte le numéro d'identifiant d'un téléphone portable et enregistre la conversation est le premier instrument. Le second instrument, le GovWare est l'équivalent du cheval de Troie qui permet de prendre contrôle d'un ordinateur infecté par lui. Une autre nouveauté est la mise en place du système informatique contrôlé par le service de surveillance qui permet une gestion des données plus efficace, notamment en ce qui concerne la communication plus sécurisée de ces données à l'autorité qui a demandé la surveillance.

Véronique Jaquet, avocate et collaboratrice scientifique à l'Office fédéral de la justice, a cependant regretté – lors de la Journée suisse du droit de la protection des données – que le travail législatif datant de 1990 ait pris du retard sur les avancées technologiques. La loi ne prévoit donc pas la surveillance des communications chiffrées et sur le réseau Internet. Par conséquent, une surveillance de WhatsApp n'est pas envisageable. Les parlementaires étaient en outre partagés vis-à-vis du respect de la protection des données. Certains saluaient le cadre qui avait été mis en place, d'autres étaient d'avis qu'il valait mieux renforcer les outils déjà existants, principalement le Code de procédure pénal plutôt que de doter le service de renseignement, supposé travailler dans l'ombre, de plus de pouvoir et ainsi plus d'accès à ses activités par le biais de voies de recours.

La protection des données en droit du travail

—

Lors de la procédure de recrutement, chaque employeur collecte et traite de nombreuses données concernant les personnes candidates. Ce traitement de données personnelles peut porter atteinte à la personnalité et présenter également un risque de discrimination pour la personne concernée. En Suisse, différentes normes légales traitent de ces aspects. En effet, le droit fondamental à ne pas être discriminé (art. 8 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999; Cst) est concrétisé par deux lois fédérales sur l'égalité (la Loi du 24 mars 1995 sur l'égalité entre femmes et hommes et la Loi du 13 décembre 2002 sur l'égalité pour les handicapés), la Loi fédérale du 19 juin 1992 sur la protection des données contribue à réaliser en particulier le droit à la protection de la sphère privée (art. 13 Cst) et le droit à ne pas subir d'atteinte illicite à la personnalité dans le cadre des rapports de travail est traité dans le Code des obligations du 30 mars 1911 (CO).

Karine Lempen, Professeure à la Faculté de droit de l'Université de Genève, a traité de la manière dont le droit antidiscriminatoire interagit avec les normes de protection des données et de la personnalité dans le cadre d'une procédure d'embauche. Lors de la procédure de sélection, l'employeur est habilité à traiter des données concernant le travailleur dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail (art. 328 et 328b CO). Selon elle, les trois régimes précités poursuivent des buts similaires et considèrent comme «sensibles» en grande partie les mêmes données. Sous réserve par exemple de la mise en œuvre de mesures positives visant l'intégration professionnelle de certains groupes sociaux sous-représentés, le droit antidiscriminatoire ainsi que la législation relative à la protection des données n'admettent que de façon restrictive le traitement de données sensibles lors du recrutement. Ainsi, dans le cadre de la procédure d'embauche, la protection des données et la protection contre les discriminations se complètent et se renforcent mutuellement.

La protection des données confiées aux assureurs

La gestion des assurances sociales et privées est sans doute un des secteurs d'activité qui génère le volume de données le plus important. Ces données présentent en grande partie un caractère très sensible dans la mesure où elles ont trait à l'état de santé des personnes assurées. Anne-Sylvie Dupont, Professeure aux Universités de Neuchâtel et Genève, a abordé le traitement des données par les assureurs à la suite d'une demande de prestations.

Afin de se déterminer en connaissance de cause, l'assureur doit réunir un certain nombre de données personnelles au sujet de l'assuré, qui sont dans leur grande majorité des données sensibles. Conformément aux règles générales de la protection des données sensibles de nature médicale, les «données ne doivent être transmises à personne, à moins que l'assuré ne consente à la communication, qu'une disposition légale n'autorise le transfert de données, voire, exceptionnellement, qu'un autre fait justificatif ne légitime la transmission des informations». Selon la Professeure Dupont, à première vue, on pourrait penser qu'il est difficile pour l'assureur d'entrer en possession des données relatives aux assurés. Toutefois, dans le cadre d'une demande de prestations formulée auprès d'un assureur, l'assuré est pratiquement transparent pour l'assureur qui ne rencontre qu'une faible résistance lorsqu'il veut obtenir des informations. Cela est notamment dû au rapport de force existant entre un assuré qui, le plus souvent, a besoin des prestations d'assurance pour survivre, et un assureur qui tient les cordons de la bourse et qui s'estime en droit de prendre le temps nécessaire et de se procurer tous les renseignements utiles pour ne les desserrer qu'à bon escient.

Elle a relevé également que les informations récoltées par un assureur social ou privé sont facilement accessibles aux autres assureurs et à certaines autorités administratives, en particulier au vu de l'obligation de collaborer imposée à l'assuré qui a demandé des prestations. En acceptant de confier ses données à un assureur, l'assuré doit ainsi admettre qu'elles puissent être mises à disposition d'un nombre important d'intervenants, dont l'identité n'est pas prévisible pour lui, en raison de la complexité de la réglementation légale et de l'absence, la plupart du temps, d'une obligation de l'informer au préalable à ce sujet. Ainsi, le nombre de personnes susceptibles de prendre connaissance de ses données personnelles est exponentiel.

En conclusion, la Professeure Dupont a exprimé qu'une séparation claire entre les prestations et le rapport médical ainsi qu'une sensibilisation des experts nommés par les assurances au sujet du principe de proportionnalité de l'expertise privilégieraient la protection des données des assurés.

Secret professionnel pour les données des patients

—

«Secret médical et confidentialité du patient: quel avenir?» Tel était le sujet de la conférence-débat de privatim à l'occasion de l'Assemblée plénière de printemps de l'association, le 17 mai 2017 à Schaffhouse.

De nombreux médecins, hôpitaux et instituts externalisent l'administration électronique, l'archivage et le traitement des données de leurs patients. Des solutions en nuage sont aussi de plus en plus utilisées à cette fin. Wolfgang Wohlers, Professeur de droit pénal à l'Université de Bâle, a établi un avis de droit sur l'externalisation des données relatives à la santé des patients. Il parvient à la conclusion qu'une externalisation n'est pas compatible avec le secret médical. Les prestataires informatiques et les services en nuage ne pourraient pas être simplement considérés comme des «auxiliaires» du médecin ou de l'hôpital en raison de leur indépendance économique et de l'absence de rapport de subordination. Le prestataire de services n'est pas non plus libre d'élargir, sans le consentement du maître du secret, p. ex. du patient, le cercle des détenteurs du secret ou des personnes «habilitées à la connaissance». C'est au contraire le patient qui décide avec qui il partage son savoir. Une exclusion de ce cercle viole ainsi le secret professionnel au sens des articles 321 et 321bis CP.

Vers un assouplissement du secret médical?

Le thème de l'externalisation a été abordé sous différents aspects. Hanspeter Kuhn, représentant de la Fédération des médecins suisses, a illustré, avec divers exemples, comment le secret médical a été assoupli par le passé. Plusieurs dispositions légales prévoient ainsi des obligations d'informer, par exemple les assureurs-maladie, l'Office fédéral de la santé publique ou le registre des tumeurs. D'après Hanspeter Kuhn, l'externalisation est une réalité vécue; sans répartition du travail, une médecine efficace est inimaginable. Il a plaidé en faveur d'une interprétation du secret médical qui tient compte de la situation effective et des besoins des patients.
Magdalena Külling, du service juridique des hôpitaux de Schaffhouse, a révélé la nécessité d'une externalisation d'un point de vue économique. Selon elle, si l'externalisation est inévitable, elle doit être réfléchie et qualifiée, car elle implique aussi une perte de contrôle.

Sous l'angle de la protection des données, Bruno Baeriswyl, préposé à la protection des données du canton de Zurich, a mis en évidence les risques supplémentaires liés à l'externalisation, comme une perte de contrôle du traitement des données, la traçabilité ou les risques d'utilisation abusive des données. Plus ces risques sont importants, plus les exigences relatives aux mesures organisationnelles et techniques sont élevées.
Au cours de la table ronde qui a suivi, des représentants des organisations de patients, du droit de la santé, du corps médical et du Préposé fédéral à la protection des données et à la transparence ont souligné l'importance de l'information du patient, notamment dans la perspective de l'introduction du dossier électronique du patient. Des adaptations légales sont indispensables, en particulier afin de fixer des standards minimaux pour l'externalisation.

Solution proposée par privatim

privatim, l'Association des préposés suisses à la protection des données, s'engage pour une meilleure protection des données relatives à la santé. On ne peut toutefois pas enrayer la tendance à l'externalisation. En guise de solution pragmatique, privatim propose une voie intermédiaire: l'externalisation doit préserver le secret médical, c.-à-d. que le prestataire externe ne peut pas avoir connaissance des données relatives à la santé. Concrètement, celles-ci ne peuvent être externalisées que sous une forme cryptée, et la clé doit rester à l'hôpital ou chez le médecin.

Médias sociaux et protection des données sous l'aspect des droits humains

—

Le Centre suisse de compétence pour les droits humains a organisé à Zurich une conférence publique au sujet de l'arrêt du 6 octobre 2015 rendu par la Cour de justice de l'Union européenne (CJUE), concernant le litige opposant M. Maximilian Schrems à la Commission de protection des données. Le jugement concerne la licéité de la transmission des données des utilisateurs de la plateforme vers les Etats-Unis. En effet, M. Schrems revendique le fait que la transmission par Facebook de ses données aux services de renseignements des Etats-Unis (NSA) est la preuve qu'elles ne sont pas protégées. Pouvons-nous utiliser Facebook, Twitter et Co en protégeant notre sphère privée?

Conformément aux règles établies par les directives européennes, le transfert de données à caractère personnel vers un Etat tiers est subordonné, à la condition que cet Etat offre un niveau de protection adéquat à l'égard de ces données. A l'origine, la Commission de l'Union européenne considérait que les Etats-Unis fournissaient un service de protection des données adéquat. La Cour a invalidé cette décision et considère que les autorités nationales irlandaises de contrôles restent chargées d'évaluer la sécurité du pays tiers en termes de protection des données. Ces autorités devaient ensuite transmettre l'affaire à la Cour car, le cas échéant, elle est seule à pouvoir invalider une décision de la Commission. En l'espèce, les Etats-Unis ne remplissent pas les exigences adéquates de protection, contrairement à ce qui avait été constaté par la Commission (Arrêt du 6 octobre 2015, Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650).
Le jugement a donné lieu à la suppression de l'accord «Safe Harbor», qui régulait le transfert des données entre l'UE et les Etats-Unis. Cet accord a été remplacé par le «Privacy Shield».

Impact de la décision

Le nouvel accord inclut notamment la possibilité du «opt out», c'est-à-dire que la personne concernée peut décider si ses données sont transmises à un tiers dans un but autre que celui qui était initialement prévu par le contrat. Il a été souligné qu'il était regrettable qu'aucune possibilité ne soit donnée afin de régler le traitement des données par le contractant même (la collecte ou la sauvegarde notamment). Le recours à des sociétés de gestion de données personnelles ne résout pas le problème.
En ce qui concerne le jugement rendu par la CJUE, celui-ci aura un impact principalement sur Facebook et ne pourra pas forcément s'appliquer à toutes les entreprises. En termes stratégiques, une entreprise dont le but est la récolte de données personnelles pour un usage commercial aura un comportement prévisible. Il existe malheureusement d'autres organismes qui ne pourront pas être interpellés à l'aide des règles de protection des données actuelles, ainsi qu'avec le «Privacy Shield». Ce sont les organismes qui essayent de dépasser les limites pouvant être atteintes avec le traitement des données: «Jusqu'où pouvons-nous aller?». Ce débat pose un problème du point de vue économique, certains intervenants ayant également mis en valeur un aspect politique. Aujourd'hui, il est largement connu que la NSA, sis aux Etats-Unis, traite des données des utilisateurs. La question est plus délicate si les données sont détenues et traitées dans d'autres pays tels que la Chine ou la Russie. Le contrôle sur les données est alors perdu. C'est une des limites du «Privacy Shield» qui n'est valable que pour les données passant vers les Etats-Unis.
Par conséquent, même avec les instruments actuels à l'échelle suisse et européenne, la protection absolue des données comme on le désirerait est difficile à réaliser. Ceci est principalement dû à un manque de moyens.

Moneyhouse SA doit adapter sa pratique de traitement des données

—

Le Tribunal administratif fédéral approuve en grande partie la plainte déposée par le Préposé fédéral à la protection des données contre le traitement des données tel que pratiqué par Moneyhouse SA. Il constate en particulier que des profils de personnalité sont créés ou traités sur le site www.moneyhouse.ch dans la mesure où des informations concernant la réputation, la situation familiale, la formation et l'activité professionnelle ainsi que les conditions de logement de particuliers y sont fournies. Moneyhouse SA est par conséquent contrainte d'obtenir l'accord express des personnes concernées avant de publier ce type de données. L'arrêt est susceptible de recours au Tribunal fédéral.

(Communiqué de presse du Tribunal administratif fédéral du 11 mai 2017; Arrêt du 18 avril 2017 dans la cause A-4232/2015).

Informations aux organes publics

Révision de l'Ordonnance sur l'accès aux documents en consultation

Depuis la mi-juin, l'avant-projet d'ordonnance modifiant l'Ordonnance sur l'accès aux documents (OAD) est en consultation. Cette modification de l'OAD fait suite à l'adoption, l'année dernière, de l'adaptation de la Loi sur l'information et l'accès aux documents (LInf) à la Convention d'Aarhus. Certaines adaptations sont nécessaires. D'abord parce que les modifications apportées par le législateur ne se sont pas limitées au seul domaine de l'environnement, mais aussi en raison des changements d'ordre procédural qui requièrent d'être précisés au niveau de l'ordonnance. Le projet propose en outre quelques ajustements de l'ordonnance qui tiennent compte de la pratique des six premières années d'application de la législation sur l'accès aux documents. La consultation dure jusqu'à la fin août.

Accès à des documents concernant les informateurs privés de la police

Dans une recommandation, la Préposée à la transparence s'est prononcée pour que la Police cantonale accorde en partie l'accès à un document révélant comment les relations entre la Police cantonale fribourgeoise et ses informateurs privés et la rémunération de ces derniers sont régies. S'agissant du budget annuel pour la rémunération des informateurs privés, elle a préconisé un accès total. Un journaliste avait formulé une telle demande, qui avait été refusée au motif que la consultation des documents sollicités compromettait la sécurité publique. Aux yeux de la Préposée, la dérogation prévue par la LInf ne justifiait pas, dans le cas concret, un refus total de la demande d'accès. La Préposée a recommandé à la Police cantonale de caviarder les passages qui tombent sous le coup de la dérogation.

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 2017