



25 juin 2018

Résumé des points essentiels du 25^e rapport d'activités

Protection des données

Le 15 septembre 2017, le Conseil fédéral a adopté le message concernant la loi fédérale sur **la révision totale de la loi fédérale sur la protection des données** et sur la modification d'autres lois fédérales. Cette révision vise à renforcer la protection des données par une amélioration de la transparence des traitements et la possibilité pour tout un chacun de mieux contrôler les données le concernant. Si nous approuvons les grandes lignes de la révision, nous avons néanmoins exprimé des réserves à l'égard du projet du Conseil fédéral, pour l'essentiel dues au fait que ce projet présente des différences terminologiques et matérielles par rapport au **règlement général de l'UE sur la protection des données** et à la convention STE 108 révisée du Conseil de l'Europe. Ces différences compliquent inutilement la situation juridique des entreprises et des autorités suisses directement soumises au règlement général de l'UE et créent une insécurité juridique. Nous nous sommes par ailleurs engagés en vain en faveur de l'adoption rapide du projet (ch. 1.1.1).

Le Conseil fédéral a chargé le Département fédéral de l'intérieur d'élaborer un projet de loi visant à faciliter **l'utilisation du numéro AVS comme identifiant personnel** par toutes les collectivités fédérales, cantonales et communales également en dehors du domaine des assurances sociales. Fin septembre 2017, le PFPDT et l'Office fédéral de la justice (OFJ) ont chargé M. David Basin, professeur de sécurité de l'information à l'EPF de Zurich d'analyser les risques liés à l'utilisation d'identifiants personnels et à l'extension prévue de l'utilisation du NAVS 13, au regard de la protection des données (ch. 1.1.2).

Le PFPDT a publié des explications concernant **l'utilisation d'outils de gestion de campagne en ligne**, dans la perspective des élections fédérales de 2019. Ces outils permettent à des groupements politiques et autres communautés d'intérêts d'organiser digitalement les contacts personnels, d'interagir avec des groupes cibles de personnes et d'intégrer des actions déterminées sur leur site internet. Nous avons précisé que les personnes concernées doivent être informées de manière complète et compréhensible sur le traitement de leurs données, avant leur enregistrement sur le site. Ces données ne pourront être utilisées que si les utilisateurs y consentent de manière explicite, libre et éclairée (ch. 1.1.3).

Les CFF nous ont informés de plusieurs projets affectant la protection des données, tels que l'utilisation de **bodycams** et le développement de nouvelles applications. Les implications juridiques de ces projets ont fait l'objet d'une analyse préalable du conseiller à la protection des données des CFF. S'agissant de **l'application mobile SwissPass**, le PFPDT a rappelé que toutes les personnes qui souhaitent voyager de manière anonyme doivent avoir la possibilité de le faire sans que leur billet coûte plus cher (ch. 1.2.1).

Fin décembre 2017, Swisscom a informé le PFPDT que des accès indus aux coordonnées d'environ 800 000 clients avaient eu lieu au cours de l'automne. Nous avons conseillé l'entreprise sur la manière



de réduire les risques et de garantir le droit à l'information de ses clients. Swisscom a effectué les clarifications nécessaires, pris les mesures qui s'imposaient et informé les clients de la **fuite de données**. Le PFPDT a pu clore ce dossier sans entreprendre de procédure formelle (ch. 1.3.2).

La création d'une **identité électronique (e-ID)** vise en premier lieu à renforcer la sécurité du droit dans les transactions électroniques. Nous suivons ce grand projet à double titre: dans le cadre de la consultation sur le projet de loi et en accompagnant deux initiatives privées (ch. 1.3.3).

Le Tribunal fédéral a confirmé la position du PFPDT s'agissant du **droit d'accès aux données secondaires des télécommunications**. Dans le cas des demandes d'accès, les fournisseurs de services de télécommunication sont tenus de fournir au requérant toutes les informations le concernant ou pouvant lui être rattachées (ch. 1.3.4).

S'agissant du projet de loi fédérale sur les mesures policières de **lutte contre le terrorisme**, la position du PFPDT s'écarte considérablement de celle de fedpol. Les dispositions concernant les mesures policières sont réglées dans plusieurs lois fédérales. Il est donc difficile d'avoir une vue d'ensemble des traitements de données personnelles dans ce domaine. Le présent projet de loi augmente encore la complexité de la situation. Nous préconisons donc l'élaboration d'une loi fédérale réglant l'activité des organes de police sur le modèle des lois cantonales existantes. Il faut impérativement régler dans quelle système d'information les données relatives aux mesures policières de lutte contre le terrorisme seront traitées (ch. 1.4.3).

Le PFPDT a examiné le traitement des données effectué par le Secrétariat d'État aux migrations (SEM) dans le cadre des **visas Schengen** et effectué un contrôle sur place. Dans le cadre des compétences qui lui sont attribuées par l'accord d'association à Schengen, le PFPDT a contrôlé les signalements visant la non-admission ou l'interdiction de séjour émanant du SEM en tant qu'utilisateur final du système d'information Schengen (SIS) (ch. 1.4.6 et 1.4.7).

En tant que membre associé, la Suisse a fait l'objet de sa **troisième évaluation Schengen** au début de l'année 2018. Cette évaluation porte sur tous les domaines de la coopération Schengen: contrôles frontaliers aux aéroports, rapatriement / renvoi de ressortissants d'États tiers en séjour illégal, utilisation du système d'information Schengen SIS II / SIRENE, politique commune en matière de visas, coopération entre les autorités policières et traitement des données à caractère personnel. Les travaux ont été coordonnés par l'Office fédéral de la justice (OFJ), en collaboration avec la Direction des affaires européennes (DAE). Le PFPDT y a contribué par son expertise dans le domaine du droit de la protection des données (ch. 1.4.5).

L'externalisation du traitement de données à des prestataires externes à la branche est en expansion dans le domaine de l'assurance-maladie comme ailleurs. Le PFPDT a enquêté sur un cas dans lequel le prestataire a ouvert la correspondance entre les assurés et leur assureur (ch. 1.6.3). Nous avons invité Swisscom Health et la Caisse des médecins à mieux informer les patients sur leur site Internet au sujet de l'externalisation (ch. 1.5.3).

Plusieurs assurances-maladie proposent des **applications pour la santé et des programmes de bonus**. Nous avons vérifié si les assurés mettent volontairement à disposition des données concernant leur santé et si les exigences de la protection et de la sécurité des données sont respectées. Le PFPDT a ouvert une procédure d'établissement des faits concernant le programme de bonus « Helsana+ » de la caisse-maladie Helsana. Constatant l'absence de base légale, il a recommandé à la société Helsana Assurances complémentaires SA d'abandonner le traitement de données issues de l'assurance de base et porté l'affaire devant le Tribunal administratif fédéral (ch. 1.6.4).



Les **systèmes biométriques d'enregistrement du temps de travail et de contrôle d'accès** (par ex. enregistrement du temps de travail au moyen d'empreintes digitales) sont de plus en plus utilisés dans le secteur de la restauration. Or les données biométriques sont sensibles et ne doivent être traitées qu'avec la plus grande retenue (ch. 1.7.4). Les systèmes de navigation embarqués à bord de véhicules de service et d'autres **appareils dotés d'un GPS** semblent de plus en plus utilisés à des fins de surveillance du personnel. Nous avons reçu de nombreuses questions de personnes concernées pendant l'année sous revue. Ce type de surveillance n'est autorisé que s'il est conforme aux exigences du droit sur la protection des données et à celles du droit du travail (ch. 1.7.3). Tout employeur devrait, dans un souci de transparence, édicter un règlement régissant l'utilisation des moyens informatiques par son personnel, et y indiquer les droits et les devoirs de chacun. Cette façon de faire permettrait d'éviter des conflits pendant les rapports de travail et à l'issue de ces derniers, tout en contribuant à **faciliter le départ en cas de résiliation des rapports de travail** (ch. 1.7.2).

Depuis avril 2017, les entreprises américaines peuvent se faire certifier au **Swiss-US Privacy Shield** (bouclier de protection des données personnelles), qui leur garantit un niveau de protection des données adéquat. Pendant l'année sous revue, le PFPDT a accompagné la mise en œuvre du Swiss-US Privacy Shield et publié un **guide destiné au public**. Cette brochure informe sur les obligations des entreprises certifiées, les droits des personnes concernées et la manière dont ces dernières peuvent déposer une réclamation. La première évaluation du bouclier Suisse-US sera effectuée en automne 2018, en même temps que la deuxième évaluation du bouclier de protection des données UE-États-Unis (ch. 1.8.1 et 3.2).

Le PFPDT a ouvert une procédure d'établissement des faits à l'encontre de la société de recouvrement de créances **EOS Suisse SA**, à la suite d'une **fuite de données**. Les patients de médecins et de dentistes suisses ont été particulièrement affectés. Dans nos avis publiés, nous avons rappelé aux professionnels de la santé qu'ils ne peuvent transmettre à des tiers que les données de leurs patients qui sont effectivement nécessaires à la facturation ou au recouvrement. La transmission injustifiée de données médicales à des tiers est pénalement punissable (ch. 1.8.2).

L'entreprise de publicité APG/SGA nous a demandé d'évaluer, sous l'angle de la protection des données, une plateforme destinée à la **publicité ciblée sur des applications utilisant des données de localisation**. Ce type de plateforme permet de traiter un grand nombre de profils de déplacement et de données de localisation pendant une durée indéterminée, ce qui permet d'identifier relativement facilement les personnes concernées. Le PFPDT a donc proposé des mesures ciblées. En outre, lors de l'installation d'applications tierces, l'utilisateur doit être informé de manière complète et transparente du traitement des données et y consentir expressément. Il doit également avoir la possibilité de révoquer en tout temps son consentement (ch. 1.8.4).

Le PFPDT est en contact avec la **régie publicitaire Admeira**, appartenant à Ringier, à la SSR et à Swisscom. Les personnes concernées doivent pouvoir s'opposer à la transmission de leurs données personnelles à des fins publicitaires. Le PFPDT a conseillé Swisscom sur ses devoirs d'information à l'égard de ses clients en relation avec les nouvelles dispositions sur la protection des données. Les personnes concernées doivent être en mesure en tout temps de reconnaître les flux de données et les analyses de transactions (ch. 1.8.5).

La mise en œuvre des nouveaux standards dans la lutte mondiale contre la fraude et la soustraction d'impôts se poursuit. La Suisse collecte des données depuis 2017 dans le cadre de **l'échange automatique de renseignements relatifs aux comptes financiers (EAR)**. Ces données seront échangées pour la première fois en 2018. L'Assemblée fédérale a approuvé la mise en œuvre de l'EAR avec une



première série d'États, dont les États-membres de l'UE, en 2016. Le Conseil fédéral a adopté le message concernant la mise en œuvre de l'EAR avec 41 autres États partenaires en juin 2017. Le PFPDT a signalé que plus de 30 de ces États ne disposent pas d'un niveau de protection des données adéquat et qu'en conséquence des garanties supplémentaires s'imposent (ch. 1.9.1).

Les intéressés doivent souvent révéler de nombreuses informations personnelles dans les **formulaires d'inscription relatifs à la location d'un appartement**. Nos explications indiquent quelles informations le bailleur est en droit de requérir et quelles questions sont illicites au regard de la protection des données (ch. 3.2).

Les dispositions du **règlement général sur la protection des données (RGPD)** de l'UE sont dans de nombreux cas directement applicables aux entreprises suisses qui traitent des données de citoyens de l'UE ou qui offrent des biens ou des services sur le territoire de l'UE. Nous avons rassemblé des informations exhaustives sur notre site Internet et publié un **guide** détaillé qui renseigne les entreprises sur leurs nouvelles obligations et les particuliers sur leurs droits en matière de protection de la sphère privée (ch. 3.2).

Principe de la transparence

Le PFPDT a mené en 2017 un **essai pilote visant à accélérer la procédure de médiation** et à réduire le nombre de cas pendants. Le rapport d'évaluation montre que les mesures prises ont permis d'atteindre les objectifs fixés et que cet essai pilote a par conséquent été un succès. Au vu des résultats positifs, la nouvelle méthode sera intégrée dans la gestion ordinaire des procédures (ch. 2.3.1).

Le projet d'ordonnance d'exécution de la nouvelle loi sur le renseignement contenait une disposition qui excluait pratiquement tous les documents du **Service de renseignement de la Confédération (SRC)** du champ d'application de la loi sur la transparence. Cette disposition, que nous avons critiquée, a été abandonnée après la consultation (ch. 2.4.1).

Pendant l'année sous revue précédente, le PFPDT s'était prononcé contre la restriction du principe de la transparence dans le projet « **Organisation de l'infrastructure ferroviaire** » (**OBI**) (ch. 2.3.1 du 24^e rapport d'activités). Le Tribunal fédéral a jugé que les informations sur la mise en danger et la perturbation des transports publics enregistrées dans une banque de données de l'Office fédéral des transports (OFT) devaient être communiquées et rejeté le recours de l'autorité qui entendait refuser l'accès à ces informations à un journaliste (ch. 2.4.2 du présent rapport). Fin mai 2018, le Parlement a décidé d'exclure du champ d'application de la loi sur la transparence l'activité de surveillance de l'OFT en matière de sécurité.

Le rapport annuel peut être téléchargé en format PDF ou être commandé auprès de l'OFCL, Vente de publications, 3003 Berne (No d'art. 410.025.f). Commande par Internet : <http://www.bundespublikationen.admin.ch>