

23^e Rapport d'activités 2015/2016

Préposé fédéral à la protection
des données et à la transparence



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2015/2016
du Préposé fédéral à la protection
des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence est tenu de fournir périodiquement à l'Assemblée fédérale un rapport sur son activité (art. 30 LPD). Le présent rapport couvre la période du 1^{er} avril 2015 au 31 mars 2016.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ce rapport est également disponible sur Internet (www.leprepose.ch)

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bundespublikationen.admin.ch

No d'art. 410.023.d/f

Table des matières

Avant-propos	7
1. Protection des données	11
1.1 Droits fondamentaux	11
1.1.1 Protection des données dans le cadre d'une collecte de signatures.....	11
1.1.2 Utilisation du numéro AVS en tant qu'identifiant universel	13
1.1.3 Registre national d'adresses	14
1.1.4 Projet MARS de l'Office fédéral de la statistique et de l'Office fédéral de la santé publique.....	15
1.1.5 Prise de position sur le cadre légal relatif aux données publiques en libre accès.....	16
1.1.6 Guide relatif aux mesures techniques et organisationnelles de la protection des données	17
1.2 Protection des données – Questions d'ordre général ...	19
1.2.1 Examen des faits concernant le SwissPass	19
1.2.2 Examen des faits concernant l'Internet gratuit des CFF	20
1.2.3 Surveillance privée des fans de football sur le domaine public	22
1.2.4 Stockage centralisé de photos de clients par des stations de ski	23
1.2.5 Communication de données personnelles à l'étranger dans la lutte contre le dopage.....	25
1.2.6 Révision des ordonnances sur l'énergie et sur l'approvisionnement en électricité	25
1.2.7 Procédure d'établissement des faits: plainte pénale pour violation de l'obligation de collaborer.....	26
1.2.8 Publication du numéro de châssis par l'OFROU	27
1.3 Internet et télécommunication	29
1.3.1 Etablissement des faits concernant Windows 10	29
1.3.2 Analyse des données de clients auprès d'opérateurs de télécommunication à des fins d'offres personnalisées.....	29
1.3.3 Accès des applications aux données	30
1.3.4 Révision de la loi sur les télécommunications.....	31
1.4 Justice/Police/Sécurité	33
1.4.1 Révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication	33
1.4.2 Loi fédérale sur le renseignement.....	34

1.4.3	Systèmes d'information de l'Administration fédérale des douanes.....	35
1.4.4	Communication de données sur les voyageurs aériens au Service de renseignement de la Confédération.....	35
1.4.5	Contrôle des logfiles auprès du Corps des gardes-frontière en tant qu'utilisateur final du Système d'information Schengen	37
1.5	Santé et recherche	38
1.5.1	Dispositions d'exécution de la loi fédérale sur le dossier électronique du patient	38
1.5.2	Etablissement des faits auprès du service médical de la Confédération ...	40
1.5.3	Refus de renseignements sur les données de santé d'un enfant.....	41
1.6	Assurances	42
1.6.1	Contrôle des services de réception de données des assureurs-maladie ...	42
1.6.2	Facturation dans le domaine SwissDRG – que peut-on transmettre au médecin-conseil?	43
1.6.3	Suppression des données auprès des assurances-accidents	45
1.6.4	Ordonnance sur la surveillance de l'assurance-maladie sociale – projet BAGSAN	45
1.6.5	Ordonnance sur la compensation des risques dans l'assurance-maladie	47
1.7	Secteur du travail	49
1.7.1	Contrôle de sécurité relatif aux collaborateurs (dans le domaine privé)....	49
1.7.2	Bureau de communication pour lanceurs d'alerte (whistleblowing) de la Confédération	50
1.8	Économie et commerce	51
1.8.1	Safe Harbor: arrêt de la Cour de justice de l'Union européenne et conséquences pour la Suisse.....	51
1.8.2	Bases légales des compteurs intelligents (smart metering) en Suisse	54
1.8.3	Carte-client du commerce de détail.....	54
1.8.4	Échanges de contenus sur Internet et droits d'auteur – révision de la loi sur le droit d'auteur	55
1.8.5	Éclaircissements dans le domaine des agences de renseignement économique et de renseignement en matière de crédit: Moneyhouse	57
1.8.6	Mise en œuvre des droits d'accès et des droits d'opposition à propos d'un vendeur d'adresses	59
1.8.7	Appels publicitaires illicites à partir d'un centre d'appels.....	59
1.9	Finances	60
1.9.1	Traitement de données client chez Postfinance	60
1.9.2	Communication de données à des autorités fiscales étrangères	61

1.9.3	Assouplissement de l'assistance administrative pour les données volées	66
1.9.4	Banques et droit d'accès	66
1.10	International	68
1.10.1	Coopération internationale	68
2.	Principe de la transparence	76
2.1	Demande d'accès	76
2.1.1	Départements et offices fédéraux	76
2.1.2	Services parlementaires	77
2.1.3	Ministère public de la Confédération	77
2.2	Demandes en médiation	78
2.3	Consultations des offices et autres prises de position	79
2.3.1	Coopération au sein du groupe de travail Transparence et révision partielle de la loi sur la transparence	79
2.3.2	Organisation de l'infrastructure ferroviaire	80
2.3.3	Libre accès aux données publiques / Open Government Data (OGD).....	81
2.3.4	Révision de l'ordonnance sur l'énergie et de l'ordonnance sur l'approvisionnement en électricité	82
2.3.5	Loi sur l'information et l'accès aux documents du canton de Fribourg	83
2.4	Varia	84
2.4.1	Conférence internationale des commissaires à l'information 2015	84
2.4.2	Relations avec les préposés cantonaux à la transparence	85
3.	Le PFPDT	86
3.1	Dixième Journée de la protection des données	86
3.2	Publications du PFPDT durant l'exercice	87
3.3	Statistique des activités du PFPDT du 1 ^{er} avril 2015 au 31 mars 2016.....	89
3.4	Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence	92
3.5	Statistique des demandes d'accès présentées auprès du Ministère public en vertu de l'art. 6 de la loi sur la transparence	101
3.6	Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence	102
3.7	Nombre de demandes de médiation par catégories de requérants	103
3.8	Secrétariat du PFPDT	104
4.	Liste des abréviations	106

Avant-propos

Il y a dix ans, le 1^{er} juillet 2006, la loi fédérale sur la transparence entrain en vigueur. Cette loi était et est appelée à jouer un rôle primordial dans le fonctionnement de notre État de droit. Son objectif est en effet de promouvoir la transparence quant à la mission, l'organisation et l'activité de l'administration, notamment en garantissant l'accès du public aux documents officiels. Les processus de décision de l'administration doivent être transparents afin de contribuer à renforcer la confiance des citoyens et citoyennes en leurs institutions publiques. La loi fédérale sur la transparence est ainsi, avec la loi fédérale sur la protection des données, l'un des éléments du bon fonctionnement d'un État démocratique respectueux des droits et des libertés fondamentales. Et c'est d'ailleurs à raison que le législateur a confié au préposé fédéral à la protection des données et à la transparence, le soin de veiller à l'application de la loi au travers de la médiation.

La mise en application de cette loi ne s'est pas faite sans difficulté. Il a fallu et il faut continuer à se battre contre les réticences de certaines administrations à répondre positivement aux demandes d'accès ou leur tendance à recourir aux motifs d'exception prévus par la loi sans examen approfondi et sans motivations fondées. Un autre frein préoccupant résulte de la politique qui consiste à exiger du demandeur le versement d'émoluments trop élevés. Le changement de paradigme voulu par le législateur devient cependant progressivement réalité et je l'espère, est devenu un mouvement irréversible. Il demeure certes encore fragile, notamment en raison des velléités de certains à vouloir au travers de propositions législatives spécifiques restreindre la portée de la loi, en particulier en introduisant des exceptions pour les activités de surveillance de certaines autorités publiques ou en soustrayant du principe de transparence certaines catégories de documents officiels.

La conduite et le fonctionnement de la procédure de médiation demeure un casse-tête pour le préposé du fait de délais irréalistes et de ressources insuffisantes. Les travaux pour une révision de la loi fédérale sur la transparence sont en cours. Ils seront révélateurs du niveau d'engagement notamment de l'administration en faveur de la transparence des autorités. Gageons que cette révision permettra de corriger les défauts de jeunesse de la loi et que le Conseil fédéral attribuera des ressources supplémentaires pour permettre le traitement des demandes de médiation dans un délai raisonnable par rapport aux attentes des demandeurs d'accès.

Depuis son entrée en vigueur, la loi sur la transparence a atteint un degré de notoriété significatif au sein de l'opinion publique. Le nombre de demandes d'accès dans l'administration fédérale et le nombre de demandes en médiation déposées auprès du préposé fédéral ne cessent d'augmenter. Cette loi permet ainsi à toute personne de déterminer elle-même quelle information elle souhaite obtenir. L'administration

n'est plus seule à décider de ce qui doit être rendu public. Aujourd'hui, les autorités fédérales sont, par exemple, tenues sur demande de renseigner et de fournir des documents sur l'utilisation des impôts, sur des projets informatiques ayant échoué ou sur des affaires de corruption. Le principe de transparence est ainsi devenu un instrument percutant à disposition de la société.

2016 est certainement une année charnière pour la protection des données. Les travaux de réforme du cadre juridique au sein de l'Union européenne sont en passe d'aboutir. Ces textes contribuent à renforcer le droit de la protection des données et permettent d'avoir un même régime pour l'ensemble des pays de l'Union européenne et de l'Espace économique européen, renforçant les droits des personnes concernées, la transparence des traitements, les obligations des responsables de traitement et les mécanismes de mise en œuvre et de coopération entre autorités de protection des données. Une autre réforme importante se termine, celle de la révision de la Convention du Conseil de l'Europe dont l'objectif est également de renforcer les droits des personnes concernées et l'effectivité de la protection des données au travers des obligations des responsables de traitement, des compétences et pouvoirs des autorités de protection des données ou des mécanismes de mise en œuvre de la Convention.

Ces réformes auront un impact certain et incontournable sur la révision en préparation de la loi fédérale sur la protection des données. Dans l'intérêt non seulement des droits des personnes concernées, mais également des entités et des entreprises qui traitent des données et donc de la place économique suisse, j'attends de cette révision globale que tout en mettant en œuvre la Convention 108, elle permette, si ne ce n'est un alignement, tout au moins un rapprochement étroit avec le cadre de l'Union européenne. J'attends également que cette révision débouche sur un réel renforcement du droit à l'autodétermination informationnelle et permette à tout un chacun de garder et d'exercer effectivement la maîtrise sur les données qui le concerne. Cela passe par de nouveaux droits pour les personnes concernées, l'introduction d'une action collective, le renversement du fardeau de la preuve, une responsabilité objective du fait du traitement et des obligations au chef des responsables de traitement, notamment obligation de mise en conformité par rapport aux exigences de la loi, annonce des violations de données, évaluation des risques, recours aux technologies de la protection des données.

Elle doit également permettre un renforcement des compétences et des moyens notamment d'investigation du préposé fédéral. Des sanctions dissuasives doivent être introduites en cas de violation de la loi. Les traitements qui présentent un risque élevé quant au respect de la vie privée doivent être soumis à des conditions strictes telles qu'autorisation préalable ou certification obligatoire. Je vise en particulier l'exploitation de mégadonnées qui débouche sur le profilage prédictif

des individus. Je pense également à des traitements entraînant la surveillance des personnes notamment aux moyens de technologies particulièrement invasives, comme le recours aux drones ou l'utilisation de systèmes biométriques. Dans un monde où les données ne connaissent pas le principe de souveraineté et de territorialité, il est en effet fondamental d'éviter des régimes de protection trop disparates. C'est aussi à ce prix que la Suisse pourra se positionner comme État fort en matière de traitement et de conservation des données et créera les conditions d'une société moderne ouverte aux progrès et aux innovations technologiques tout en garantissant à ses citoyens le respect de leurs droits et libertés fondamentales.

Plus que jamais, je plaide pour la mise en place d'un cadre juridique contraignant au niveau mondial. Une étape importante en ce sens peut être franchie avec la révision en cours de la Convention 108 du Conseil de l'Europe et avec l'adhésion à ce traité d'États non membres du Conseil de l'Europe. L'arrêt de la Cour de justice de l'Union européenne du 4 octobre 2015 déclarant que le système du «Safe Harbor» ne permettait pas d'assurer un niveau de protection des données adéquat face à l'accès massif et incontrôlé des autorités américaines aux données transmises aux entreprises américaines, a démontré la nécessité d'un système fort pour assurer la protection des données lors du transfert des données vers des États sans protection. Cette décision me paraît aussi renforcer la nécessité de parvenir à l'adoption d'un instrument universel de protection des données. Gageons que la nomination d'un rapporteur spécial des Nations Unies à la vie privée contribuera également à réaliser cet objectif.

La modernisation de notre cadre juridique est indispensable, mais pas suffisant. Les exigences légales doivent pouvoir être concrétisées dans les différents secteurs concernés (code de conduite) et implémentées dans les systèmes et les technologies d'information et de communication. La règle devrait être celle de la protection des données par défaut. La technologie est en soi capable de réaliser ces exigences. Certaines entreprises rechignent cependant à agir en ce sens. Je plaide dès lors pour une véritable politique d'incitation à développer et à recourir à des technologies favorables à la protection des données. La confiance des personnes concernées passe par ce type de technologie et en particulier par la possibilité de recourir à des systèmes sûrs de chiffrement des données excluant l'existence de porte dérobée. La sécurité des systèmes est aussi un facteur de diminution de la criminalité.

Parallèlement, la formation et l'éducation au numérique doivent être érigées en priorité et faire l'objet de programmes nationaux atteignant l'ensemble des couches de la population. La connaissance et la maîtrise du fonctionnement des technologies, de leurs avantages et leurs risques sont une condition d'une utilisation consciente, responsable, informée et libre de celles-ci.

Notre société se trouve à la croisée des chemins: l'Homme numérisé et quantifié, l'intelligence artificielle, l'internet des objets, l'émergence des voitures et des robots intelligents, les paiements sans contact et la disparition du numéraire, l'exploitation des mégadonnées et le profilage comportemental et prédictif sont autant de développements qui peuvent évoluer de manière positive ou négative. Lorsque je lis qu'une personne en Suède souhaite digitaliser tout ce que est dans ses poches (clés, téléphone mobile, portefeuille, carte bancaire) pour les transférer dans une puce unique placée sous sa peau, je m'inquiète de l'évolution, avec la complicité le plus souvent inconsciente des personnes, de nos sociétés libérales et démocratiques vers une société de surveillance permanente aboutissant à l'abrutissement et la manipulation des individus, donc à la fin de l'autonomie individuelle et du libre arbitre. Si en effet ces nouveaux développements technologiques ne respectent pas les valeurs fondamentales de la société, les droits de l'homme et en particulier le droit à la dignité et à la non-discrimination, ils risquent d'entraîner rapidement des dommages irréversibles et une mise sous tutelle des personnes. La société numérique se doit d'être démocratique et conforme aux droits et libertés fondamentales sous peine de déboucher sur une nouvelle forme de dictature.

Il y a urgence à agir et à fixer les règles de comportements qui éviteront que des algorithmes décident ce qui est bien pour nous, déterminent ce que nous devons savoir ou penser et comment nous devons agir et nous comporter. Il n'est pas encore trop tard, mais le temps presse pour construire un monde où la technologie soit utilisée pour le bien de l'humanité! Les droits fondamentaux doivent également être garantis dans le monde numérique. Cela passe par un nouveau contrat social basé sur la confiance et la coopération des individus. Ceux-ci doivent être des partenaires et non des adversaires ou de simples biens de consommation. Pour ce faire, il faut mettre en place un cadre juridique assurant la compatibilité des technologies avec la démocratie et l'exercice effectif du droit à la protection des données. La révision de la loi fédérale sur la protection des données est une opportunité à saisir pour réaliser cet objectif. Elle doit être accompagnée d'un vaste débat démocratique et participatif sur la société numérique en Suisse.

Jean-Philippe Walter

Préposé fédéral ad intérim

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Protection des données dans le cadre d'une collecte de signatures

À la demande de la Chancellerie fédérale, nous avons explicité les exigences légales concernant l'utilisation des données collectées dans le cadre de l'exercice des droits politiques (collecte de signatures). Conformément au principe de finalité, les données personnelles recueillies à l'appui d'une initiative populaire ou d'un référendum ne peuvent être utilisées qu'aux fins de l'initiative ou du référendum. L'utilisation de ces données pour une autre finalité, par exemple l'envoi d'une lettre d'information, n'est licite que si la personne concernée y consent librement et de manière explicite.

La section des droits politiques de la Chancellerie fédérale nous a priés de décrire, du point de vue du droit de la protection des données, les exigences concernant l'utilisation, par des personnes privées, des données personnelles recueillies dans le cadre d'une collecte de signatures effectuée à l'appui d'une initiative ou d'un référendum.

La collecte de signatures à l'appui d'un référendum ou d'une initiative populaire ou l'utilisation des données personnelles collectées dans le cadre de l'exercice des droits politiques constituent des traitements de données personnelles soumis à la loi fédérale sur la protection des données (LPD) et à ses principes généraux. Les données recueillies dans le cadre de l'exercice des droits politiques doivent être considérées comme sensibles au sens de la LPD, car elles fournissent des indications sur les opinions ou les activités politiques des personnes concernées. La LPD confère une protection accrue à ce type de données, la qualification de données sensibles appelant notamment une rigueur toute particulière dans l'application des principes généraux de protection des données.

Le soutien à un référendum ou à une initiative populaire implique une collecte et un traitement de données personnelles – prévu par la loi sur les droits politiques – visant essentiellement à vérifier la validité de la signature. La personne qui appose sa signature à l'appui d'un référendum ou d'une initiative populaire ne doit en principe pas s'attendre à l'utilisation de ses données pour l'envoi d'informations ou encore la prospection pour la collecte de fonds, etc. (principe de finalité). Une telle utilisation de données personnelles nécessite un (nouveau) motif justificatif, à savoir le consentement de la personne concernée, un intérêt privé ou public

prépondérant, ou la loi. En l'occurrence, seul le consentement des signataires entre en considération pour justifier une utilisation de ses données à d'autres fins qu'à l'appui de l'initiative, respectivement à son aboutissement.

Pour qu'un consentement soit considéré comme valable, la LPD exige que la personne concernée exprime sa volonté librement et après avoir été dûment informée (consentement libre et éclairé). S'agissant de données sensibles ou de profils de la personnalité, le consentement doit être au surplus explicite. L'utilisation à d'autres finalités des données personnelles collectées dans le cadre d'une initiative (qui doivent être considérées comme des données sensibles) nécessite par conséquent un consentement libre, éclairé et explicite.

Dans le cas concrètement présenté par la Chancellerie, le formulaire de récolte de signatures comportait une petite case – apposée à droite de la signature – qui devait être cochée dans le cas où le signataire n'accepterait pas l'utilisation de ses données pour l'envoi d'informations; la non-acceptation nécessite une action de la personne concernée, sous forme de case à cocher (opt-out). Au-dessus de ladite case figurait en petits caractères «pas d'infos svp (cocher)» [en allemand: «Schick mir bitte keine weiteren Infos (ankreuzen)»]. La question qui se posait en particulier était de savoir si l'absence de case cochée pouvait être considérée comme consentement valable du point de vue de la LPD, pour l'envoi d'informations.

Nous avons estimé que le mode d'acquisition du consentement ne répondait pas aux exigences de la LPD. L'information quant à l'utilisation faite de ces données sensibles n'était d'une part pas suffisamment claire. D'autre part et surtout, l'absence de case cochée ne saurait ici valoir consentement, puisque le traitement de données sensibles nécessite un consentement explicite. La signature apposée à côté du nom et de l'adresse ne se rapporte qu'au soutien de l'initiative ou du référendum en question et non à une autre utilisation de ces données personnelles.

En outre, nous estimons qu'une case à cocher opt-in apposée avant la signature ne permettrait pas d'éviter les risques d'abus, une case pouvant aisément être cochée par un tiers. Cette solution ne représente donc pas à notre avis une solution sûre et conforme aux principes de protection des données. Le principe de sécurité exige en effet que les données personnelles soient protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Dans ce contexte, nous conseillons aux comités d'initiative ou de référendum de requérir le consentement explicite des personnes intéressées par le biais d'une feuille séparée ou au moyen d'une nouvelle signature, ou d'une autre manière qui garantisse de façon suffisamment sûre que les personnes concernées ont consenti librement et explicitement à une utilisation de leur données à d'autres fins, après avoir été dûment informées sur les finalités du traitement.

1.1.2 Utilisation du numéro AVS en tant qu'identifiant universel

Durant l'année sous revue, nous avons requis du Conseil fédéral qu'il prenne une décision de principe sur l'utilisation généralisée du numéro AVS en dehors du secteur des assurances sociales. Nous considérons que seul un numéro sectoriel serait à même de limiter les risques de mise en relation abusive de données.

En marge de notre participation à un groupe de travail chargé d'examiner l'élaboration de bases légales pour l'utilisation d'un identifiant personnel administratif dans la cyberadministration (cf. notre [22^e rapport d'activités](#), chiffre 1.1.7), nous avons adressé au Chef du Département fédéral de l'intérieur nos préoccupations quant à l'utilisation généralisée du numéro AVS en dehors du secteur des assurances sociales.

Compte tenu de l'évolution préoccupante dans ce domaine et des risques accrus d'atteintes qui en résultent pour la sphère privée des personnes concernées, nous avons estimé opportun d'attirer l'attention du Conseil fédéral sur cette problématique, afin qu'il se prononce clairement en faveur ou en défaveur de l'utilisation systématique du numéro AVS en dehors du secteur des assurances sociales, respectivement qu'il envisage un réexamen législatif de cette disposition afin d'en restreindre la portée.

L'Office fédéral des assurances sociales (OFAS) a été chargé de rédiger une note de discussion pour le Conseil fédéral. Lors de la consultation des offices, nous avons relevé que la note de discussion se limite à proposer des modifications de la Loi fédérale sur l'assurance-vieillesse et survivants (LAVS) visant à préciser les conditions d'utilisation du numéro AVS dans l'application du droit cantonal (status quo plus) et n'apporte aucune réelle solution pour contenir l'utilisation croissante du numéro AVS en dehors des assurances sociales. Nous avons également rappelé que si aucune mesure n'est prise pour contrôler l'utilisation de ce numéro, sa fiabilité risque d'être remise en cause.

Le Conseil fédéral a pris acte de la note de discussion et a chargé le Département fédéral de l'intérieur d'étudier la question de l'utilisation du numéro AVS plus à fond, notamment la possibilité de l'utiliser comme identificateur unique pour la cyberadministration, et de soumettre au Conseil fédéral le résultat de son analyse et la suite des travaux d'ici le premier semestre 2016.

Nous considérons que seul un numéro sectoriel serait à même de limiter les risques de mise en relation abusive de données tout en répondant aux besoins de l'administration et des citoyens (exactitude des données, absence de confusion, qualité des données, etc.) puisqu'il dispose des mêmes fonctionnalités que le numéro AVS.

Contrairement à l'opinion de certains, un numéro sectoriel est facile à mettre en place et peu coûteux. Nous avons relevé qu'un numéro sectoriel a été introduit dans plusieurs domaines – comme celui du dossier électronique du patient – car les risques ont été bien perçus, garantissant ainsi un meilleur équilibre entre la protection de la sphère privée et les besoins de l'administration. De plus, l'ère du Big Data et de la cybercriminalité impose que l'utilisation de cet identifiant à tout va soit fondamentalement repensée et qu'elle mériterait une vision plus globale que celle d'une administration ou d'un canton.

1.1.3 Registre national d'adresses

Nous faisons partie d'un groupe de travail chargé d'examiner diverses variantes de mise en œuvre du projet de registre national d'adresses pour les administrations publiques. Il s'agit d'analyser les solutions proposées, notamment leur faisabilité, leur compatibilité avec la protection des données, leur coût et leurs conséquences.

Après avoir renoncé à l'échange automatique des adresses entre la Poste et les services de contrôle des habitants, le Conseil fédéral étudie actuellement la possibilité de créer un registre central des adresses à l'usage des pouvoirs publics. Plusieurs solutions sont possibles. Le registre central serait réalisable dans le cadre des structures étatiques en place: la banque de données pourrait être alimentée par les plateformes cantonales existantes, ou bien se fonder sur des plateformes de la Confédération, comme la banque de données de la statistique de la population ou la banque de données UPI «Unique Person Identification» exploitée par la Centrale de compensation de l'AVS.

Le Conseil fédéral a chargé le Département fédéral de justice et police d'examiner de plus près ces solutions, notamment leur faisabilité, leur compatibilité avec la protection des données, leur coût et leurs conséquences. Nous faisons partie du groupe de travail institué pour approfondir les variantes proposées. L'examen a débuté par une analyse de faisabilité sur le plan technique. Les réflexions se poursuivront avec l'examen juridique des variantes retenues. Nous continuons à nous engager activement afin de garantir que les exigences de protection des données soient prises en compte dans le cadre de ce projet.

1.1.4 Projet MARS de l'Office fédéral de la statistique et de l'Office fédéral de la santé publique

Lors de la procédure de consultation des offices, nous avons eu l'occasion de prendre position sur deux nouvelles dispositions de l'Ordonnance sur l'assurance-maladie (OAMal). Celles-ci règlent les détails de la collecte, du traitement, de la transmission et de la publication des données dans le cadre du projet Modules Ambulatoires des Relevés sur la Santé (MARS).

Pour rappel, l'Office fédéral de la statistique (OFS) est chargé par la loi sur la statistique fédérale de produire des statistiques d'intérêt public. Dans le domaine de la santé, l'OFS a pour mission spécifique d'établir les bases statistiques nécessaires à l'examen du fonctionnement et des effets de la loi fédérale sur l'assurance-maladie (LAMal). Les relevés statistiques fédéraux doivent être étendus à la médecine ambulatoire, afin d'obtenir des données sur l'ampleur des soins dans ce domaine, sur les raisons du recours à ces soins (diagnostics) ainsi que sur les prestations et sur les coûts du secteur ambulatoire. L'OFS effectue également des relevés auprès des fournisseurs de prestations afin de pouvoir transmettre des données aux instances qui sont chargées d'une mission légale de surveillance.

Conformément à l'art. 59a LAMal (respectivement l'ancien article 22a al. 4 LAMal), le Conseil fédéral doit régler les détails de la collecte, du traitement, de la transmission et de la publication des données, dans le respect du principe de la proportionnalité. Nous avons régulièrement insisté sur la nécessité d'une concrétisation rapide de cet article. En décembre 2014, l'Office fédéral de la santé publique (OFSP) et l'OFS nous ont soumis le projet des nouvelles dispositions de l'ordonnance (OAMal). Suite à une entrevue entre l'OFSP, l'OFS, l'Office fédéral de la justice (OFJ) et nous-mêmes, le projet a été remanié, puis soumis en mars 2015 en procédure de consultation des offices.

Nous avons pris position notamment sur les catégories de données traitées, la notion d'appariement de données et celle de pseudonymisation; nous avons également apporté des remarques concernant la mention des destinataires des données et celui d'un délai de conservation. En outre, il nous est apparu indispensable de rappeler que le traitement des données effectuées dans le cadre du projet MARS doit respecter le principe de proportionnalité et l'anonymat des patients doit être garanti.

Parallèlement aux modifications apportées à l'OAMal, un règlement de traitement est en cours d'élaboration auprès de l'OFS; celui-ci règle les aspects techniques de l'utilisation du numéro AVS, des appariements de données, de la pseudonymisation et de l'anonymisation, ainsi que du procédé cryptologique et du Key Management.

Au vu de la nature sensible des données personnelles collectées, nous restons particulièrement attentifs au développement du projet et veillons à ce que les exigences de la protection des données soient pleinement respectées.

1.1.5 Prise de position sur le cadre légal relatif aux données publiques en libre accès

Les Archives fédérales nous ont priés de prendre position du point de vue de la protection des données dans le cadre d'une consultation des offices relative aux données publiques en libre accès (Open Government Data OGD).

Le 16 avril 2014, le Conseil fédéral a adopté la stratégie de libre accès aux données publiques (stratégie OGD) jusqu'à 2018. Cette stratégie a été élaborée par l'Unité de pilotage informatique de la Confédération et sa mise en œuvre confiée début 2015 aux Archives fédérales qui établissent actuellement les bases conceptuelles de ce projet. Nous avons donc été priés de prendre position du point de vue de la protection des données sur les conditions-cadres des données publiques en libre accès.

Les portails OGD servent généralement à la publication de données factuelles ou de données agrégées et préalablement anonymisées. Toutefois, selon les circonstances, la délimitation par rapport aux données personnelles peut être difficile à faire. C'est essentiellement ce point que nous avons mis en évidence dans notre prise de position.

Ainsi, même si elles ne permettent à première vue aucune identification, les données ne sont pas considérées comme anonymisées lorsque la référence aux personnes peut être aisément reconstituée (par ex. par des tiers), en particulier par l'association à d'autres données. Elles constituent des données personnelles conformément à la loi sur la protection des données. Par conséquent, les conditions relatives au traitement de données personnelles par des organes de la Confédération doivent être respectées. L'organe de la Confédération qui gère le portail OGD doit garantir par des mesures techniques et organisationnelles qu'aucune donnée personnelle ne sera publiée. Si malgré tout, il faut que des données personnelles soient exceptionnellement publiées dans le cadre des OGD, l'organe fédéral responsable doit avoir une base légale à cette fin.

Le responsable d'un portail OGD doit examiner régulièrement si les données qu'il publie sont toujours anonymes en raison du développement technologique et des possibilités de réidentification grandissantes. Les projets OGD doivent dès lors prévoir ce type de procédures de contrôle. - Nos remarques en matière du principe de transparence sur le libre accès aux données publiques se trouvent au chiffre 2.3.3 du présent rapport d'activités.

1.1.6 Guide relatif aux mesures techniques et organisationnelles de la protection des données

Notre guide concernant les mesures techniques et organisationnelles a fait l'objet d'une révision terminologique. Les données personnelles sont classifiées selon leur sensibilité, ce qui permet de les traiter et les protéger de manière adéquate. La classification des données en trois niveaux est comparable à celle de la protection de l'information et peut être transposée au niveau des mesures techniques et organisationnelles.

Nous avons actualisé le guide relatif aux mesures techniques et organisationnelles de la protection des données (désormais également disponible en anglais) sur le plan de la terminologie: partant des définitions légales ou des niveaux de risque associé à leur traitement, les données personnelles ont été classifiées en fonction de leur nature: données «non sensibles», «sensibles» et «ultrasensibles». En termes de niveau de risque, les données sensibles et les profils de la personnalité au sens de la loi fédérale sur la protection des données (art. 3 let. c et d LPD) appartiennent au niveau de risque «élevé» (classe «sensible»), tandis que les données personnelles non sensibles recouvrent les niveaux de risque «moyen» et «minimal» (classe «non sensible»). Le niveau de risque «très élevé» (classe «ultrasensible») est quant à lui réservé aux données dont l'abus peut mettre en danger la vie ou l'intégrité corporelle des personnes concernées.

Cette classification ne doit pas être confondue avec celle de la protection de l'information (INTERNE/CONFIDENTIEL/SECRET), qui vise à protéger les intérêts nationaux conformément à l'Ordonnance sur la protection de l'information et à la future Loi sur la sécurité de l'information. L'utilisation du label CONFIDENTIEL pour désigner des données personnelles de classe «sensible» est inappropriée et doit être absolument évitée.

Les deux types de classifications présentent cependant des similitudes de sorte qu'une mise en parallèle des mesures techniques et organisationnelles de protection associées à chaque niveau de classification (non sensible/INTERNE, sensible/CONFIDENTIEL, ultrasensible/SECRET) permet de gagner en simplicité, efficacité et clarté.

À partir de la classe «sensible», respectivement CONFIDENTIEL, un chiffrement des transmissions et des mémorisations est ainsi obligatoire. Ceci est valable pour n'importe quel système de gestion de données, tels que les systèmes de gestion électronique des affaires (GEVER), mais aussi les solutions complémentaires fournissant une assistance automatisée à la classification des données/informations, ou les possibilités offertes par l'infonuagique en matière d'hébergement de (méga)données.

Enfin, on peut noter que l'exigence de classification des données/informations fait partie intégrante de la majorité des standards internationaux de sécurité des informations/données. À titre d'exemple, citons la mesure A8.2 (Classification de l'information) de la norme ISO/CEI 27001:2013 et la mesure additionnelle 8.4 (Protection des échanges d'information) de la norme complémentaire ISO/CEI 27010:2015 (Communications intersectorielles et interorganisationnelles) dont l'annexe C décrit l'incontournable 'Traffic Light Protocol (TLP)', ainsi que la mesure P02.3 ('Data Classification Scheme') du référentiel ISACA/COBIT 5:2012 ou encore le processus OSP-21 ('Information Quality and Compliance Assessment') du cadre The Open Group/O-ISM3:2011. Le gouvernement américain n'est pas en reste avec son 'National Institute of Standards and Technology (NIST)', dont la publication spéciale SP 800-53R4:2013 comprend l'annexe J intitulée 'Privacy Control Catalogue' qui définit par exemple la mesure SE-1 ('Inventory of Personally Identifiable Information'). Le guide SP 800-122:2010 est par ailleurs entièrement consacré à la protection de la confidentialité des données personnelles, en définissant notamment des niveaux d'impact (bas-moyen-haut) sur la confidentialité des données personnelles, dont un des facteurs déterminants n'est autre que la sensibilité des données considérées.

Le Royaume-Uni a en outre introduit à partir du 2 avril 2014 une nouvelle politique appelée 'Government Security Classifications', dont la classification de base OFFICIAL comprend le sous-ensemble OFFICIAL-SENSITIVE (ex CONFIDENTIAL), potentiellement complété par les descripteurs :PERSONAL ou :COMMERCIAL pour identifier la présence de données sensibles de personnes physiques ou morales. En théorie, la classification peut même aller jusqu'à la granularité de chaque paragraphe du document globalement classifié, de façon à pouvoir envisager une anonymisation assistée par ordinateur, par exemple dans le cadre d'une demande d'accès selon la Loi fédérale sur le principe de la transparence dans l'administration (LTrans).

Finalement, le futur Règlement général de protection des données de l'Union européenne va essentiellement dans la même direction avec son orientation centrée sur les données, comportant entre autre la notification obligatoire des violations de données, une évaluation d'impact relative à la protection des données, le droit à l'oubli, des sanctions (financières) plus importantes pour les traitements abusifs, ainsi qu'un encouragement à la certification et à la labellisation de certains traitements.

1.2 Protection des données – Questions d’ordre général

1.2.1 Examen des faits concernant le SwissPass

Fin 2015, nous avons procédé à un examen des faits à propos du SwissPass des CFF et de l’Union des Transports Publics (UTP). Nous avons conclu que les traitements de données effectués lors des contrôles des titres de transport n’étaient pas proportionnels et ne reposaient pas sur une base légale suffisante. Nous avons donc établi une recommandation à l’intention de l’UTP et des CFF afin de corriger les défauts constatés.

Les CFF et l’UTP nous ont informés du projet de SwissPass le 3 mars 2015, soit une semaine avant la publication du communiqué de presse. Il s’agissait d’une information purement préliminaire nous présentant les principaux aspects du projet.

Depuis le 1^{er} août 2015, tous les abonnements généraux et les abonnements demi-tarifs sont remplacés au fur et à mesure par le SwissPass. Ce dernier sert également de support pour des prestations de partenaires tels que Mobility, Publi-Bike, SuisseMobile et quelques domaines skiabiles.

Fin 2015, nous avons procédé à un examen des faits lié au SwissPass et aux traitements connexes de données. À ce propos, nous avons examiné en particulier la banque des données récoltées à la suite des contrôles. Nos constatations ont révélé les éléments présentés ci-après.

Immédiatement après l’achat d’un abonnement général ou d’un abonnement demi-tarif, les données du client sont introduites dans la banque de données centrale concernant la clientèle et les abonnements. Au cours du contrôle, le personnel des CFF pose sur le SwissPass un appareil de lecture qui contient une copie locale des données de l’abonnement afin de scanner ce dernier. Les données d’identité, le type d’abonnement et sa durée de validité (valable, en partie valable, non valable) apparaissent sur l’écran de l’appareil de lecture. Les données de contrôle, composées entre autres de l’heure, du numéro de train et du numéro de la course ainsi que du lien avec le numéro de la carte SwissPass, sont téléchargées sur la banque des données de contrôle, où elles sont conservées pendant 90 jours.

Les CFF ont été chargés par l’UTP de la prospection du marché et de la gestion des banques de données du SwissPass; ils sont également responsables du traitement des demandes d’accès. Dans la mesure où il n’existe pas d’objection manifeste (opting out) de la part du client, les données de clients et de prestations sont aussi utilisées à des fins de marketing. Les données de contrôle elles-mêmes ne sont pas utilisées à des fins de marketing et ne sont pas communiquées à des tiers.

Notre examen des faits nous a permis de conclure que les traitements de données effectués dans le contexte de la banque des données de contrôle n'étaient pas proportionnels et ne reposaient pas sur une base légale suffisante. Nous avons donc émis une recommandation à l'intention de l'UTP et des CFF dans laquelle nous exigeons l'effacement immédiat des données récoltées lors des contrôles et la cessation de l'exploitation de la banque de données de contrôle. Nous leur avons en outre transmis deux propositions d'amélioration concernant la formulation des conditions générales de l'abonnement général et de l'abonnement demi-tarif, notre but étant de garantir que les clients soient informés de manière claire et appropriée sur l'utilisation de leurs données à des fins de marketing et sur leur droit de s'opposer à cette utilisation.

Le 4 janvier 2016, nous avons envoyé notre rapport final à UTP et aux CFF. Ces deux organismes ont accepté notre recommandation et les propos d'améliorations. Nous allons examiner leur mise en œuvre encore cette année.

1.2.2 Examen des faits concernant l'Internet gratuit des CFF

Nous avons procédé à un examen des faits concernant l'offre de wifi gratuite des CFF. À cette occasion, nous avons constaté que le système présentait un certain nombre de défauts. Nous avons donc émis des recommandations, à la suite desquelles les CFF ont modifié les dispositions en matière de protection des données de ce service ainsi que la durée de conservation des données d'utilisateurs.

À l'automne 2013, nous avons déjà contacté les CFF à propos de leur offre d'accès gratuit à Internet dans certaines gares. Ils n'ont toutefois pas donné suite à notre demande visant à modifier les conditions générales régissant ce service (cf. chiffre 1.3.4 de notre [22^e Rapport d'activités](#)). À la suite de cela, nous avons donc procédé à un examen des faits auprès des CFF.

Pour pouvoir utiliser l'accès gratuit à Internet dans les gares, les clients doivent s'enregistrer. Pour ce faire, ils doivent indiquer leur numéro de téléphone mobile, accepter les conditions générales et demander le code d'accès. L'enregistrement est effectif dès l'introduction du code transmis par SMS. Les CFF ont publié sur leur site Internet les conditions générales relatives au «free wifi CFF», accompagnées d'informations plus détaillées.

Au moment où nous avons procédé à notre examen des faits, les données relevées dans le contexte de l'accès Internet gratuit des CFF n'étaient utilisées que pour la prestation du service en question, pour le traitement des demandes de

renseignements ainsi que dans le contexte de la loi fédérale sur la surveillance par poste et télécommunication (LSCPT). Contrairement aux conditions générales existant alors, les données n'étaient traitées ni pour améliorer les flux de personnes, ni pour analyser les comportements des clients en matière de déplacement, ni pour générer des annonces spécifiques dans le domaine de l'information aux clients. Les données relevées en vertu de la LSCPT n'étaient effacées qu'au bout de neuf mois. Au cours de nos recherches, les CFF ont adapté leurs conditions générales une première fois.

Forts du résultat de nos recherches, nous avons émis deux recommandations qui concernaient toutes deux le traitement des données en relation avec la LSCPT. Nous avons recommandé aux CFF de ne traiter que les données qui tombaient effectivement sous le coup de la LSCPT et en particulier de ne plus relever les données «adresse IP de destination» et «port de destination». Nous leur avons demandé en outre de conserver les données d'utilisation et les données accessoires des communications uniquement aussi longtemps que cela est prévu la loi, à savoir six mois et non pas neuf mois. De plus, nous avons fait aux CFF deux propositions d'amélioration. D'une part, nous avons suggéré l'élaboration d'une procédure consignée par écrit, régissant le traitement des demandes de renseignements. D'autre part, nous leur avons demandé d'adapter leurs conditions générales aux traitements de données effectivement réalisés.

Les CFF ont accepté notre seconde recommandation ainsi que nos deux propositions d'amélioration. Par contre, ils ont indiqué ne pas pouvoir se conformer à notre première recommandation car le Service de surveillance de la correspondance postale et des télécommunications (le SSCPT) leur avait fortement conseillé de continuer à enregistrer les données mentionnées ci-dessus pour les autorités de poursuite pénale.

Nous sommes toutefois d'avis que la journalisation de «adresse IP de destination» et «port de destination» n'est pas prévue en l'état par la LSCPT. Néanmoins, en raison de l'actuelle révision de la LSCPT, nous renonçons pour l'instant à soumettre ce point aux autorités compétentes. En conséquence, nous avons clos l'examen des faits, mais nous nous sommes expressément réservé le droit de revenir ultérieurement sur la question de la journalisation de «adresse IP de destination» et de «port de destination» et, le cas échéant, de requérir par voie judiciaire l'application de nos conclusions (cf. égal. le chiffre 1.4.1 du présent rapport d'activités).

1.2.3 Surveillance privée des fans de football sur le domaine public

Lorsque les fans de football sont secrètement filmés sur le domaine public, leur personnalité peut être violé illicitement. Une telle mesure pourrait éventuellement être légitimée par le fait qu'elle est exécutée dans le cadre d'une intervention policière ou seulement dans le cas d'un incident.

Un projet de la Swiss Football League a fait les gros titres au printemps 2015: des groupes de supporters doivent être accompagnés par des personnes privées et filmés en secret lorsqu'ils allaient assister à des matchs extérieurs, afin d'obtenir des preuves en cas de débordements, de dégradations, etc. La Swiss Football League nous a contactés en début d'année afin de clarifier quelques questions relevant du droit de la protection des données. De manière générale, nous avons pris position comme suit.

La mesure prévue, qui consiste à faire accompagner des supporters par des personnes privées réalisant des prises de vue en cachette lors de matchs à l'extérieur, est problématique du point de vue de la protection des données: il s'agit d'une surveillance vidéo privée sur le domaine public, qui enfreint notamment les principes de proportionnalité et de transparence. Toutes les personnes qui se trouvent dans le champ de prise de vue – indépendamment d'incidents concrets – sont filmées, même si elles se comportent correctement. Et les personnes concernées ne savent pas que leur image est capturée. Ainsi, cette approche peut constituer une atteinte illégale à leurs droits de la personnalité. On peut donc au moins s'interroger sur la validité de l'utilisation de ces prises de vue en tant que preuves dans une procédure pénale. Par ailleurs, les personnes concernées peuvent engager une procédure civile et exiger par exemple la suppression des images ainsi que des dommages et intérêts. Par conséquent, cette mesure n'atteint pas ses objectifs.

On peut évaluer la situation sous un autre angle lorsque l'une des approches suivantes est respectée:

1. La mesure est convenue avec la police et intégrée directement dans un dispositif de sécurité. La personne assurant la prise de vue remplit une fonction policière sur mandat de la police. La question de savoir si cela est possible dépend des bases juridiques cantonales ou communales, et doit être examinée avec le corps de police compétent.
2. Si l'on filme sur une base purement privée, c'est-à-dire sans concertation avec la police, la caméra ne peut être activée qu'en cas d'incident, et seul ledit incident peut être filmé. Ainsi, on peut éviter au moins que des personnes au

comportement correct soient filmées sans motif. On peut ainsi supposer que cette démarche serait proportionnée et qu'elle se justifierait par un intérêt prépondérant.

1.2.4 Stockage centralisé de photos de clients par des stations de ski

Avec la fonction PhotoCompare de Skidata, les contrôles de forfaits de ski entraînent une atteinte aux droits de la personnalité des clients plus importante que la procédure habituelle. Son utilisation doit donc être limitée aux forfaits à validité longue. Les clients doivent être informés spécifiquement et les données ne peuvent être conservées que sur de courtes périodes.

Les contrôles d'accès pratiqués par de nombreuses stations de ski au moyen de forfaits d'abonnement avec photo soulèvent certaines questions du point de vue de la protection des données. C'est pourquoi nous nous sommes plusieurs fois intéressés à ce sujet dans le passé (voir par exemple notre [22^e rapport d'activités 2014/2015](#), chiffre 1.2.3). Entre-temps, ces systèmes ont été perfectionnés et complétés par des fonctions supplémentaires. Les stations de ski doivent notamment avoir la possibilité de contrôler, même a posteriori, les utilisations de forfaits.

C'est à cela que sert la fonction de comparaison de photos de la société Ski Data. À chaque passage de tourniquet, une photo de contrôle du skieur est prise. Elle peut être comparée au moment souhaité à la photo de référence stockée dans la base de données centralisée des abonnements. Ainsi, les stations de ski ont la possibilité de reporter les contrôles en cas de forte fréquentation, et de les effectuer à un moment plus favorable. Par ailleurs, cette fonction permet de découvrir et de sanctionner les abus de forfaits systématiques et durables. Les stations de ski justifient en effet le recours à cette fonction par l'augmentation du nombre de cas d'abus. À la demande de personnes concernées et du fabricant, nous avons analysé cette fonction et sommes parvenus à la conclusion suivante:

Avec la fonction de comparaison de photos, les contrôles de forfaits de ski entraînent une atteinte aux droits de la personnalité des clients plus importante que les contrôles d'accès traditionnels. En forçant le trait, on peut dire que tous les abonnés sont généralement soupçonnés et que les données sont stockées de manière préventive, ce qui est toujours délicat sur le plan du droit de la protection des données. C'est pourquoi le recours à cette fonction doit respecter les points suivants, en plus des conditions générales qui s'appliquent aux systèmes de contrôle d'accès (voir notre [22^e rapport d'activités 2014/2015](#), chiffre 1.2.3):

L'utilisation de PhotoCompare se justifie uniquement pour les abonnements de valeur élevée, c'est-à-dire notamment pour les forfaits saisonniers ou hebdomadaires. En revanche, il convient d'y renoncer pour les forfaits de courtes durées. Le système de Ski Data autorise ce type de paramétrages afin que seules certaines catégories de forfaits fassent l'objet de photographies de contrôles.

En cas d'utilisation de PhotoCompare, les skieurs doivent être préalablement informés dans les conditions générales (CG) ou dans des dispositions spécifiques sur la protection des données, ainsi que sur place par des panneaux d'avertissement bien visibles, du fait qu'ils peuvent être photographiés en passant le tourniquet. Cette précaution sert non seulement au respect du principe de transparence, mais également, selon notre expérience, à l'acceptation du système par les personnes concernées.

Les photographies de contrôle ne peuvent être conservées que quelques jours. À cet égard, la durée de stockage peut être réglée de manière individuelle dans le système. La sauvegarde des photographies de comparaison pendant toute la durée de validité du forfait, pratiquée par quelques stations de ski, peut se révéler problématique dans certaines circonstances: dans le cas des forfaits saisonniers ou annuels, cela entraîne une durée de conservation allant de plusieurs mois à un an. Cette très longue durée se justifie certes par le fait que les abus et les fraudes répétés peuvent ainsi être découverts et documentés, mais cela suppose de conserver les données de tous les titulaires de forfaits de longue durée (c'est-à-dire aussi de ceux qui agissent correctement). La valeur ajoutée de cette mesure nous paraît donc incertain.

À l'aide de la fonction de comparaison de photos, l'utilisation des forfaits peut être contrôlée en détail chaque jour (ou au moins plusieurs fois par semaine), ce qui permet de découvrir immédiatement les abus (qui, selon les conditions tarifaires que nous connaissons de la plupart des stations de ski, entraînent la suppression immédiate de l'abonnement). C'est pourquoi une conservation de longue durée des images des personnes qui se comportent correctement n'est pas nécessaire. Les opérateurs doivent donc supprimer ces photographies et ne peuvent continuer de stocker que celles qui documentent un abus éventuel. Avec les autres données enregistrées, des modèles d'utilisation suspects sur une longue durée peuvent être découverts et clarifiés de manière ciblée, sans une atteinte aux droits de la personnalité de l'ensemble des clients.

1.2.5 Communication de données personnelles à l'étranger dans la lutte contre le dopage

En Suisse, l'entrée en vigueur de la loi fédérale sur l'encouragement du sport et de l'activité physique a permis de créer une base légale pour la lutte contre le dopage. La loi règle également la transmission de données personnelles entre les organes de lutte antidopage. Cette protection doit être assurée par des conventions contractuelles en cas de transmission dans un pays n'offrant pas un niveau suffisant de protection.

Ces dernières années, nous avons à plusieurs reprises attiré l'attention sur la problématique de la transmission de données dans des pays n'offrant pas un niveau adéquat de protection des données (cf. [20^e rapport d'activités](#) 2012/2013, chiffre 1.2.6 avec autres renvois). L'Agence mondiale antidopage (AMA) de Montréal n'était soumise ni à la législation canadienne sur la protection des données, ni à celle de la province de Québec. Nous avons par conséquent demandé que les fournisseurs de données soient tenus d'assurer le niveau de protection d'une autre manière, p. ex. contractuellement. L'AMA nous a contacté concernant cette exigence et nous a présenté un concept visant à garantir le niveau de protection des données. Lors des négociations, nous avons demandé certaines adaptations, qui ont été acceptées par l'AMA, de sorte que des données personnelles de lutte contre le dopage peuvent être transmises à l'AMA à Lausanne dans le respect de la législation suisse.

1.2.6 Révision des ordonnances sur l'énergie et sur l'approvisionnement en électricité

Nous avons examiné la proportionnalité de la publication de données personnelles sur Internet par un organe fédéral dans le cadre de notre prise de position relative à la révision des ordonnances sur l'énergie et sur l'approvisionnement en électricité. Nous avons conclu que l'extension prévue de la publication aboutissait à une trop faible amélioration de la transparence et requis que cet élargissement soit abandonné.

Le projet d'ordonnance prévoyait de publier, pour toutes les installations de production d'électricité obtenant une rétribution, une liste contenant les informations suivantes: nom du producteur, lieu de l'installation, sources d'énergie utilisées, catégorie et type d'installation, puissance, production réalisée, montant de la rétribution, date d'inscription, date de mise en service et durée de la rétribution.

Selon le droit en vigueur, seules les données personnelles sur les installations d'une puissance de raccordement de plus de 30 kVA qui sont soumises à l'obligation

d'enregistrement des installations, de l'électricité produite et de la garantie d'origine peuvent être publiées. Toutes les installations affichant une puissance de raccordement inférieure ont auparavant été mentionnées sur la liste sous une forme anonyme avec NPA, localité et canton.

Nous avons examiné la proportionnalité du projet d'extension de la publication des données personnelles dans le cadre de la procédure de participation. L'évaluation de la proportionnalité du traitement des données doit comparer l'atteinte à la personnalité des personnes concernées à la finalité du traitement en question. Si un organe fédéral publie des données personnelles sur Internet, il faut que cette démarche soit nécessaire pour atteindre l'objectif fixé, parce qu'elle s'effectue sans l'approbation des personnes concernées et qu'elle va au-delà des dispositions légales. C'est pourquoi une partie de la population, craignant les abus de leurs données personnelles sur Internet, adopte une approche restrictive. Cependant, les personnes concernées ne peuvent influencer la publication par les organes fédéraux telle qu'elle est prescrite par la loi.

Selon le rapport explicatif, la publication de la liste nominative des rétributions doit améliorer la transparence sur l'utilisation du supplément perçu par les utilisateurs finaux. Du point de vue du droit de la protection des données, on peut se demander si la publication supplémentaire des données personnelles des producteurs qui perçoivent une rétribution sous forme de montants modestes permet d'atteindre une amélioration suffisante/appropriée de la transparence. Sur la liste des bénéficiaires de la rétribution à prix coûtant du courant injecté de 2013, la nouvelle règle aurait multiplié par plus de quatre le nombre de données personnelles, tandis que le volume attribuable des contributions n'aurait augmenté que de huit pour cent. Selon nous, l'atteinte aux droits de la personnalité d'un si grand nombre de personnes concernées pour une utilité si faible n'était donc pas adaptée. C'est pourquoi nous avons pu convaincre l'Office fédéral de l'énergie de renoncer à l'extension de la publication sur Internet.

1.2.7 Procédure d'établissement des faits: plainte pénale pour violation de l'obligation de collaborer

Les personnes traitant des données ont un devoir de collaborer dans les procédures que le PFPDT engage pour l'établissement des faits. La violation de cette obligation est punissable. Nous avons déposé plainte contre des personnes en infraction.

Après que des requêtes de citoyens eurent attiré notre attention sur un traitement de données potentiellement illicite, nous avons ouvert en la matière une procédure d'établissement des faits au sens de l'article 29 de la loi sur la protection des

données (LPD). Cette décision a été communiquée par écrit au responsable des traitements. Après réception du courrier d'ouverture, celui-ci nous a contactés, en premier lieu par téléphone. Mais il ne nous a jamais transmis la prise de position écrite que nous lui avons demandée en même temps que d'autres documents, et n'a plus réagi à nos courriers d'avertissement. Il a rompu tout contact avec nous, et un dernier courrier envoyé en recommandé nous a été retourné avec la mention «Non retiré».

Un tel comportement nous empêche d'exercer une activité de surveillance efficace. Nous l'avons donc considéré comme un refus de collaborer à l'établissement des faits et avons déposé plainte contre les responsables sur la base de l'art. 34, al. 2, let. b LPD.

Effrayé par l'ouverture de la procédure pénale, le responsable du traitement nous a finalement contactés et nous a soumis les documents écrits demandés. Nous avons donc pu exécuter et clore l'établissement des faits. Suite à notre déclaration de désintérêt, l'autorité compétente en matière de poursuite pénale a clos la procédure.

1.2.8 Publication du numéro de châssis par l'OFROU

À la suite de l'examen d'une demande émanant de l'OFROU, nous avons établi que le numéro VIN des véhicules constituait une donnée personnelle régie par la loi sur la protection des données. De ce fait, l'OFROU a besoin d'une base légale s'il désire communiquer ces numéros. Il conviendrait auparavant d'examiner avec précision si les principes généraux de la protection des données permettent une telle communication.

L'Office fédéral des routes (OFROU) nous a consultés pour savoir si le numéro VIN (vehicle identification number, ou numéro de châssis) constitue ou non une donnée personnelle au sens de la loi sur la protection des données. L'OFROU lui-même avait reçu plusieurs demandes émanant de personnes désirant obtenir les listes complètes des VIN.

Les constructeurs automobiles donnent à chaque voiture particulière un numéro d'identification propre qui permet de déterminer sans équivoque non seulement le véhicule, mais aussi chacun des éléments qui le composent. Pour ce qui est des véhicules agricoles ou des remorques, il se peut, dans de rares cas, que les VIN soient attribués plusieurs fois. Le numéro VIN sert essentiellement à identifier un véhicule.

La question se posait de savoir quels efforts le maître du fichier ou un tiers devrait objectivement déployer afin d'identifier un détenteur des véhicules sur la base du VIN communiqué par l'OFROU. Il convenait aussi à ce propos de prendre en considération l'intérêt de la personne traitant les données ou du tiers à l'identification.

À l'OFROU, les numéros de châssis sont enregistrés dans le système d'information relatif aux véhicules (MOFIS), avec les données des détenteurs. Même si l'office ne publie que le numéro, sans indication du détenteur, le destinataire des informations sait qu'il s'agit de véhicules immatriculés en Suisse. Grâce aux moyens techniques actuels, il est permis de supposer qu'en particulier les destinataires actifs dans le secteur automobile peuvent faire un lien avec une personne identifiable, dans ce cas le détenteur du véhicule. Ainsi, les importateurs et les garagistes disposent déjà des numéros de châssis de leurs véhicules ou peuvent le demander au constructeur lui-même. De plus, on ne peut exclure un intérêt du destinataire à l'identification du détenteur. Il suffit en outre qu'une identification soit possible grâce à une partie des informations (en l'occurrence le numéro de châssis) pour qualifier les données en question de données personnelles.

Le numéro de châssis permet d'identifier sans ambiguïté le fabricant du véhicule car une partie de ce numéro est constituée d'un code qui lui est attribué. Une recherche très rapide parmi les différents sites Internet permet de déterminer quel VIN appartient à quel fabricant.

Nous sommes parvenus à la conclusion que le VIN constitue une donnée personnelle régie par la loi sur la protection des données. De ce fait, l'OFROU a besoin d'une base légale pour pouvoir communiquer ce numéro. Avant de créer éventuellement cette base légale, l'OFROU devrait évaluer soigneusement si les principes généraux de la protection des données (proportionnalité, finalité, etc.) permettent une telle communication.

1.3 Internet et télécommunication

1.3.1 Etablissement des faits concernant Windows 10

Durant l'exercice sous revue, Microsoft a lancé son système d'exploitation Windows 10. Dans le cadre de ce lancement, notre attention s'est portée sur les traitements de données y relatives, en particulier les aspects concernant l'information des personnes concernées et leur consentement.

Suite au lancement de Windows 10, nous avons étudié en détail le traitement des données par Microsoft. Nous avons ainsi constaté que, lors du processus d'installation de Windows 10, les «paramètres express» qui sont proposés aux utilisateurs dans la fenêtre de démarrage rapide activent par défaut presque tous les transferts de données et les accès qui s'y rapportent. Sont ainsi notamment transmis à Microsoft des données de localisation, les réseaux WLAN reconnus dans l'environnement des utilisateurs de Windows 10, les historiques de navigation et de recherche, les entrées vocales, les entrées de dessin à main levée et au clavier, ainsi que les données de feedback et de diagnostic.

Sur la base de ce constat, nous avons engagé une procédure d'établissement des faits et adressé à Microsoft un questionnaire sur les traitements de données liés à Windows 10. Il s'agissait de déterminer le type et l'étendue des données transmises, et de savoir si les personnes concernées avaient été préalablement informées de manière suffisamment claire et ont eu l'occasion de consentir au traitement des données. - Lors de la rédaction de ce rapport l'établissement des faits était encore en cours.

1.3.2 Analyse des données de clients auprès d'opérateurs de télécommunication à des fins d'offres personnalisées

L'entreprise Cablecom a révisé ses conditions générales. Certaines dispositions étant formulées de manière peu claire, nous avons procédé à quelques éclaircissements auprès de cette entreprise et lui avons demandé d'améliorer certains points.

En septembre 2015, l'entreprise upc cablecom Sàrl (ci-après Cablecom) a modifié les conditions générales applicables à ses services de divertissement et de télécommunication. Les clients ont été priés de s'annoncer dans un délai déterminé au cas où ils ne seraient pas d'accord avec les nouvelles conditions générales, dans lesquelles il était prévu que Cablecom pouvait traiter des données d'utilisateurs pour améliorer et développer ces services et personnaliser ses offres.

Nous avons donc demandé à Cablecom de nous communiquer par écrit quelles données elle traitait en détail et de quels services et offres personnalisés il s'agissait concrètement. Nous lui avons également fait remarquer que des profils de la personnalité soumis à la loi sur la protection des données sont parfois traités et que conformément aux conditions générales, ces données sont destinées à être utilisées à une autre fin. Dans ce cas, le consentement de la personne concerné doit être explicite, l'absence de réaction de la part d'un client à propos des nouvelles conditions générales ne suffit pas.

Il est ressorti de notre examen que les données d'utilisateurs correspondaient à celles qui étaient générées en relation avec l'utilisation de la TV-box «Horizon» (le décodeur TV). Lorsque les clients installent ce décodeur à leur domicile, ils sont informés à un moment donné sur leur écran que des données sont générées lors de l'utilisation de certains services. Elles sont utilisées notamment pour proposer aux clients des émissions ou films qui correspondent à leurs préférences. Nous sommes d'avis qu'il a été suffisamment satisfait au besoin de transparence étant donné que les clients peuvent en tout temps désactiver le traitement de données et les réactiver. Les clients peuvent se prononcer clairement pour ou contre le traitement de ces données.

Les paragraphes concernés des nouvelles conditions générales sont toutefois pas assez clairs et portent à confusions. Nous avons donc demandé que ces passages soient améliorés. Cablecom a apporté les précisions nécessaires sur l'utilisation des données d'utilisateurs dans une fiche d'information séparée dont le lien figure dans les conditions générales. Ces rectifications seront directement introduites dans ces conditions au cours d'une prochaine révision.

1.3.3 Accès des applications aux données

Lors de l'installation d'une application sur un smartphone, il est utile de prendre le temps d'étudier les autorisations qui sont demandées, et qui sont généralement liées à l'accès aux données.

Avant l'installation d'une application sur un smartphone, il est demandé aux utilisateurs d'accorder diverses autorisations. Celles-ci sont parfois requises pour le bon fonctionnement de l'application, mais il est également fréquent qu'elles ne soient pas indispensables, voire totalement superflues.

Le fait qu'une application de navigation ne puisse fonctionner qu'avec des informations de localisation est compréhensible. Mais d'autres apps peuvent utiliser ces données pour afficher des publicités géolocalisées, ou à d'autres fins servant davantage leur éditeur que leur utilisateur. D'une manière générale, il faut être

conscient que le prix à payer pour profiter d'applications gratuites ou bon marché réside souvent (principalement) dans nos données.

Certaines applications exigent par exemple un accès à l'appareil photo du téléphone. Souvent, le but recherché n'est pas visible au premier abord. Peut-être existe-t-il une fonction réellement utile, telle que la lecture de codes-barres, qui requiert l'appareil photo. Mais l'autorisation accordée peut permettre à l'application d'activer celui-ci à tout moment, et de prendre des clichés.

Le PFPDT a par exemple étudié de plus près une application d'examens médicaux de dépistage. Une analyse des risques est réalisée en fonction des données saisies par l'utilisateur et des examens supplémentaires peuvent être recommandés. Nous avons demandé aux développeurs des explications sur ces autorisations requises, dont la portée nous semble très large. Leur point de vue nous a semblé cohérent. L'application doit par exemple pouvoir lire, modifier et supprimer des contenus sauvegardés car les résultats peuvent être envoyés à une adresse e-mail sous forme de fichier PDF. Cependant, l'application aurait pu être programmée sans cette fonction, en faisant simplement apparaître le résultat sur l'écran de l'appareil.

Nous conseillons aux utilisateurs de bien étudier les autorisations demandées par une application afin de déterminer si elles sont utiles. De surcroît, les conditions générales, notamment la politique de confidentialité, doivent également être lues avec attention. Le traitement des données personnelles par une application doit être transparent pour l'utilisateur. Si la finalité des autorisations qui sont demandées n'est pas claire, et si l'éditeur n'est pas fiable, il convient de renoncer à l'installation de l'application.

1.3.4 Révision de la loi sur les télécommunications

Nous avons été invités par l'Office fédéral de la communication à prendre position dans le cadre de la révision de la loi sur les télécommunications. Nos remarques sur le projet de loi concernaient notamment les services d'annuaires et d'appels d'urgence.

Le projet de loi sur les annuaires téléphoniques prévoit que les clients ne pourront choisir qu'entre une publication ou aucune publication de l'entrée dans l'annuaire, mais ne pourront déterminer le canal de publication. Les clients qui ne souhaitent pas publier leur adresse et leur numéro de téléphone sur Internet ont pour l'instant comme unique possibilité le blocage complet de leur adresse, bien qu'ils soient prêts à les rendre disponibles via les autres canaux. La publication des données des annuaires sur Internet est un sujet délicat sur le plan de la protection des données, car elle est souvent perçue comme un blanc-seing donné au traitement des données à diverses fins. Ainsi, il existe certains opérateurs de sites Internet, anonymes

et peu sérieux, qui accèdent aux données des annuaires « officiels » et publient des informations fausses ou obsolètes, sans permettre la correction ou la suppression de ces données. Nous avons donc demandé d'ancrer dans la loi une possibilité de choisir le canal de publication. Malheureusement, l'Office fédéral de la communication (OFCOM) n'a pas retenu nos remarques.

Comme nous l'avons déjà indiqué à l'OFCOM lors de plusieurs consultations des offices, les entrées des annuaires, notamment celles avec astérisque, ne doivent pas être utilisées pour la publicité directe en raison du principe de la finalité. Ce point a déjà été établi dans le message de 2003 relatif à la modification de la loi sur les télécommunications: « La notion de services basés sur les annuaires exclut en revanche l'utilisation de données d'annuaires pour faire de la publicité directe ». Nous constatons que le système actuel d'opposition à la publicité par insertion d'un astérisque dans l'annuaire téléphonique n'est pas satisfaisant, car les opérateurs publicitaires ne le respectent pas tous, et qu'un certain flou règne autour de l'importance de l'astérisque. Pour empêcher que l'entrée dans l'annuaire soit utilisée à des fins de publicité directe, les clients n'ont plus qu'une seule possibilité: ne pas faire publier du tout leurs coordonnées dans l'annuaire. Cette démarche ne permet toutefois pas une véritable liberté de choix, et entraîne une diminution du nombre de personnes qui se font répertorier dans les annuaires. Nous avons donc demandé que la loi sur les télécommunications intègre une interdiction expresse de l'utilisation des entrées d'annuaire à des fins de publicité directe. Malheureusement, l'OFCOM n'a pas souhaité fixer une telle restriction explicitement dans la loi.

Concernant les services d'appel d'urgence, nous soutenons les efforts visant à imposer aux prestataires de services de téléphonie publics le routage des appels d'urgence et la géolocalisation des appelants, conditions indispensable à la réalisation efficace de leur tâche. Mais si des services d'urgence peuvent même à l'avenir activer le « location manager » de l'appelant, cela entraînerait des problèmes avec le droit fondamental de la protection de la sphère privée. Nous avons donc proposé de transférer à l'Office fédéral la compétence pour standardiser l'utilisation/agencement d'une application d'appel d'urgence et pour déterminer dans quelle mesure on peut accéder à l'appareil à des fins de géolocalisation. L'OFCOM ne souhaitait pas intégrer dans la loi une possibilité de mettre en place une application standardisée d'appel d'urgence, mais a néanmoins prévu la disposition concernant l'accès aux fonctions de localisation sans l'autorisation de l'utilisateur. Nous suivrons la mise en œuvre dans l'ordonnance afin d'assurer le maintien d'une protection appropriée de la sphère privée des utilisateurs.

1.4 Justice/Police/Sécurité

1.4.1 Révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

Durant l'année sous revue, nous avons été invités par les Commissions des affaires juridiques des deux Conseils à participer aux séances concernant la révision totale de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Le thème portait notamment sur la durée de conservation des données accessoires et sur l'enregistrement de l'historique Internet.

L'année dernière, les Commissions des affaires juridiques du Conseil national et du Conseil des États nous ont invités à participer aux séances visant à élaborer le projet de la LSCPT entièrement révisée. À cet égard, nous avons rappelé notre position, déjà maintes fois exprimée, selon laquelle une atteinte à un droit fondamental protégé par la Constitution requiert des bases juridiques clairement définies, tant formelles que matérielles.

Dans ce contexte, nous avons souligné que la disposition proposée pour les renseignements visant à identifier les auteurs d'infractions sur Internet était trop ambiguë et pouvait permettre la saisie et l'enregistrement des historiques d'utilisation d'Internet pendant toute la durée de la relation commerciale. Avec une telle extension disproportionnée de la durée de conservation, l'atteinte aux droits fondamentaux ne pourrait plus être justifiée.

Concernant la durée de conservation des données accessoires, nous avons là aussi rappelé que depuis le début du projet législatif, nous estimons que l'extension de la durée de sauvegarde à douze mois n'est pas nécessaire car une durée de six mois offre déjà des conditions largement suffisantes pour les poursuites pénales (cf. [22^e rapport d'activités](#) 2014/2015, chiffre 1.4.4). Nous sommes d'accord avec la demande de la Commission du Conseil des États, qui vise à maintenir l'actuelle durée de conservation de six mois tant pour le domaine des postes que pour celui des télécommunications.

Nous suivons avec inquiétude les efforts visant à utiliser également les données accessoires pour la poursuite des infractions de droit civil (cf. chiffre 1.8.4 du présent rapport d'activités). Dans le cadre des débats sur la révision totale de la LSCPT, il nous a été régulièrement assuré que les données accessoires ne seraient sauvegardées et utilisées qu'à des fins pénales. Cette restriction nous paraît indispensable car les données accessoires sont également protégées par la Constitution, respectivement le droit fondamental au respect du secret des postes et des télécommunications.

1.4.2 Loi fédérale sur le renseignement

La loi fédérale sur le renseignement prévoit des contrôles à plusieurs niveaux et des procédures spécifiques relatives à l'acquisition des informations soumises à autorisation et à l'exploration du réseau câblé. Il s'agira de vérifier si les contrôles susmentionnés permettront effectivement de protéger les droits fondamentaux des personnes concernées. La nouvelle loi présente également quelques éléments problématiques en matière de protection des données.

Nous avons à plusieurs reprises indiqué (cf. notre [22^e rapport d'activités](#) 2014/2015, chiffre 1.4.2) que le projet de loi sur le renseignement contient encore des éléments problématiques en matière de protection des données. La loi fédérale du 25 septembre 2015 sur le renseignement contient toujours ces points préoccupants: la loi permet en effet au Service de renseignement de la Confédération (SRC) d'utiliser des aéronefs et des satellites pour observer des événements et des installations dans des lieux publics et librement accessibles et d'y effectuer des enregistrements visuels et sonores. Le SRC a également la possibilité d'infiltrer des systèmes et des réseaux informatiques afin de perturber, empêcher ou ralentir l'accès à des informations. Enfin, la loi sur la transparence ne s'applique pas à l'accès aux documents officiels portant sur la recherche d'informations au sens de la loi sur le renseignement.

34

Si les points susmentionnés peuvent constituer une atteinte importante à la sphère privée et devront faire par conséquent l'objet d'une attention particulière, nous pouvons en revanche saluer les différentes mesures de contrôle mises en place par cette nouvelle loi. Ainsi, en matière de contrôle et de surveillance du SRC, la loi sur le renseignement prévoit la création par le Conseil fédéral d'une autorité de surveillance indépendante et d'un organe de contrôle indépendant pour l'exploration radio et l'exploration du réseau câblé. Les activités du SRC sont également surveillées et contrôlées par le Conseil fédéral. Enfin, la haute surveillance parlementaire est exercée par la Délégation des Commissions de gestion et par la Délégation des finances. Le SRC est l'un des organes fédéraux les plus contrôlés. Ce cadre devrait permettre de protéger les droits fondamentaux des personnes concernées. Si tel ne devait pas être le cas, il conviendra de mettre en place d'autres mesures de surveillance du SRC.

Enfin, avant la mise en œuvre d'une mesure de recherche soumise à autorisation, celle-ci doit être autorisée par le Tribunal administratif fédéral et doit recevoir l'aval du chef du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Le chef du DDPS décide la mise en œuvre après avoir consulté le chef du Département fédéral des affaires étrangères (DFAE) et celui du

Département fédéral de justice et police (DFJP). Cette procédure s'applique également à l'exploration du réseau câblé. Ces mécanismes devraient également permettre la protection des droits fondamentaux des personnes concernées.

1.4.3 Systèmes d'information de l'Administration fédérale des douanes

Le projet de révision partielle de la loi sur les douanes contient des bases légales suffisantes pour les systèmes d'information de l'Administration fédérale des douanes traitant des données sensibles et des profils de la personnalité.

Comme nous l'avons mentionné dans notre [21^e rapport d'activités](#) 2013/2014 (chiffre 1.4.7), les dispositions relatives aux systèmes d'information de l'Administration fédérale des douanes (AFD) qui contiennent des données sensibles ou permettent d'établir des profils de la personnalité, ne répondent pas à toutes les exigences d'une base légale au sens formel. Dans le cadre de la révision partielle de la loi sur les douanes, le Département fédéral des finances a élaboré des normes relatives aux systèmes d'information de l'AFD conformes à la législation sur la protection des données. Ces normes couvrent les systèmes d'information suivants: système d'information en matière pénale, système d'information pour la gestion des résultats des contrôles douaniers, système d'information pour l'établissement d'analyses des risques, système d'information pour le soutien à la conduite, système d'information pour la documentation de l'activité du Corps des gardes-frontière et système d'information pour appareils de prise de vue, de relevé et autres appareils de surveillance.

1.4.4 Communication de données sur les voyageurs aériens au Service de renseignement de la Confédération

Durant l'année sous revue, nous avons examiné la communication de données sur les voyageurs aériens du Secrétariat d'État aux migrations au Service de renseignement de la Confédération. Nous avons pu constater que celle-ci est conforme à la protection des données. Par contre, les normes d'application doivent être complétées.

Le Secrétariat d'État aux migrations (SEM) communique les données sur les voyageurs aériens au Service de renseignement de la Confédération (SRC). La Délégation des Commissions de gestion nous a demandé de vérifier si cette communication repose sur une base légale suffisante. Pour être conforme aux exigences en matière de protection des données, les organes fédéraux ne sont en droit de communiquer

des données personnelles que s'il existe une base légale. Dans le cadre de notre analyse, nous avons constaté que les dispositions de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) peuvent seules entrer en ligne de compte en tant que base légale. Les données communiquées ne sont elles-mêmes pas des données sensibles. Par contre, le traitement de ces données personnelles dans le contexte de la sûreté intérieure et extérieure de l'État leur donne un caractère sensible et pourrait, dans certains cas, constituer des profils de la personnalité. Pour cette raison, la collecte par le SRC des données sur les voyageurs aériens et leur communication par le SEM doivent reposer sur une base légale au sens formel.

Conformément à la LMSI, le SRC recherche les informations nécessaires à l'exécution de ses tâches légales et ce même à l'insu de la personne concernée (art. 14, al. 1). La loi prévoit que le SRC peut collecter des données personnelles par le biais d'enquêtes sur l'identité ou le lieu de séjour de personnes et du relevé de leurs déplacements et de leurs contacts (art. 14, al. 2 LMSI). Cette disposition de la LMSI indique la catégorie des données collectées de même que la finalité de cette collecte. L'article 14, alinéa 1 et 2 constitue ainsi une base légale au sens formel permettant au SRC de collecter des données sur les voyageurs aériens.

En outre, sur la base de l'article 13, alinéa 1 LMSI, le SEM est tenu de fournir des renseignements au SRC. L'alinéa 2 de cette disposition stipule que le SEM doit communiquer spontanément des renseignements au SRC lorsqu'il décèle des menaces concrètes pour la sûreté intérieure ou extérieure et qu'il doit fournir des renseignements conformément à sa mission générale d'information en application de l'article 11 LMSI ou à des mandats du SRC dans des cas particuliers. L'article 11, alinéa 2 LMSI donne au Département fédéral de la défense, de la protection de la population et des sports (DDPS) la compétence de déterminer, dans une liste confidentielle, les opérations qui doivent être annoncées au SRC mais qui ne peuvent pas être publiées parce qu'elles doivent être gardées secrètes. La communication des données sur les voyageurs aériens du SEM au SRC repose également sur une base légale suffisante au sens formel.

Après avoir vérifié l'existence des bases légales au sens formel, il est nécessaire d'analyser les normes d'application. Celles-ci doivent être suffisamment précises pour que le traitement prévu respecte notamment le principe de proportionnalité. En application de l'article 4, alinéa 2 de l'ordonnance sur le Service de renseignement de la Confédération, le SEM doit communiquer spontanément et sans délai au SRC les faits et les constatations énumérés dans la liste confidentielle du DDPS visée à l'article 11, alinéa 2, LMSI. Cette liste confidentielle est soumise chaque année au Conseil fédéral pour approbation puis, pour information, à la Délégation

des Commissions de gestion (art. 11, al. 7 LMSI). Cette liste, une fois approuvée par le Conseil fédéral, peut être considérée comme une norme d'application de niveau comparable à une ordonnance du Conseil fédéral. La liste confidentielle du DDPS doit contenir la liste des données personnelles qui doivent être communiquées au SRC. Nous avons constaté que cette liste confidentielle du DDPS ne mentionne pas explicitement toutes les communications de données sur les voyageurs aériens et doit être complétée afin de constituer une base légale suffisante.

1.4.5 Contrôle des logfiles auprès du Corps des gardes-frontière en tant qu'utilisateur final du Système d'information Schengen

Dans le cadre des accords d'association à Schengen, nous avons procédé à un contrôle des logfiles auprès du Corps des gardes-frontière (Cgfr) en tant qu'utilisateur final du Système d'information Schengen (SIS). L'analyse des logfiles a montré que l'accès au SIS par cet organe était conforme à la protection des données.

Dans le cadre des accords d'association à Schengen, nous effectuons annuellement des contrôles auprès des utilisateurs finaux du SIS. Nous avons ainsi procédé au contrôle des accès des collaboratrices et des collaborateurs de la région IV du Cgfr.

Nous avons effectué notre analyse à partir des logfiles du N-SIS qui nous ont été transmis par l'Office fédéral de la police. Nous avons vérifié les accès de 30 collaboratrices et collaborateurs de la région IV du Cgfr effectués pendant une semaine. Il ressort de ce contrôle qu'aucune recherche ne semblait abusive ou disproportionnée. Par conséquent, nous avons clos ce contrôle sans émettre de recommandation.

1.5 Santé et recherche

1.5.1 Dispositions d'exécution de la loi fédérale sur le dossier électronique du patient

La loi fédérale sur le dossier électronique du patient (LDEP) a été adoptée par le Parlement le 19 juin 2015. Le délai référendaire a expiré le 8 octobre 2015. L'identifiant sectoriel pour le dossier électronique du patient est donc devenu réalité. Mais de nombreux points délicats doivent encore être clarifiés.

La LDEP doit entrer en vigueur mi-2017. Elle régit les principes tels que le fait que l'identification des patients se fasse non seulement par le numéro d'assurance sociale, mais aussi via un identificateur sectoriel eHealth. Nous avons œuvré et plaidé pendant plusieurs années pour arriver à cette étape importante. Pourtant, de nombreux points déterminants ne seront clarifiés que dans les ordonnances connexes. Durant l'année sous revue, nous nous sommes exprimés en détail sur les projets présentés, dans le cadre de la consultation des offices. Parmi les principaux points de notre prise de position, on peut citer le droit de la protection des données qui s'applique aux communautés de référence et eHealth, les conditions de certification et les autorisations d'accès.

Concernant le droit de la protection des données qui s'applique aux communautés et aux communautés de référence, nous estimons que la loi sur la protection des données (LPD) s'applique au traitement de données personnelles et que nous sommes l'autorité de surveillance compétente en la matière. Cette conclusion doit être énoncée dans les commentaires relatifs à l'ordonnance. Les communautés doivent se constituer en tant que personnes morales de droit civil, indépendamment du type de participants, et la relation entre patients et communautés/communautés de référence doit être de nature privée. C'est ainsi que la LPD s'applique. Indépendamment de cette motivation purement juridique, l'application de la LPD s'impose également pour des raisons pratiques. Il est important, dans l'optique de la sécurité juridique des patients et des autres participants au système eHealth Suisse, que les mêmes dispositions de protection des données s'appliquent au dossier électronique du patient dans toute la Suisse et qu'une autorité de surveillance en garantisse l'application uniforme. En ce sens, l'application de la LPD et la surveillance par nos soins servent également de pérennisation des investissements aux communautés et communautés de référence ainsi qu'à leurs organisations d'exploitants. L'Office fédéral de la santé publique (OFSP) interviendra en tant que propriétaire du schéma de certification et devra s'assurer du respect des prescriptions de certification, en collaboration avec les certificateurs accrédités. Nous restons toutefois compétents pour la surveillance de la protection des données.

Concernant les conditions techniques et organisationnelles de certification pour les communautés et communautés de référence, nous avons regretté une focalisation excessive sur la sécurité des données et le fait que les aspects de la protection des données soient insuffisamment pris en compte. Une telle approche contredit d'une part la disposition de la LDEP qui prévoit une certification tenant compte à la fois de la protection et de la sécurité des données et d'autre part, le respect de la protection des données représente une exigence centrale du dossier électronique du patient. Il convient d'accorder à ce point un poids suffisant dans le cadre des prescriptions de certification.

De même, nous avons pris position sur la possibilité de donner à des groupes de professionnels de la santé l'accès au dossier électronique du patient. À cet égard, nous avons souligné que les dispositions d'ordonnance ne prévoyaient pas l'accès de ces groupes de manière restrictive, comme nous l'avions demandé. Au contraire, elles doivent donner lieu à des autorisations globales de groupe. Selon nous, l'octroi d'autorisations représente une déclaration d'intention qui ne peut avoir un effet juridique que si elle est émise à l'égard d'une personne ou d'un service possédant une personnalité juridique. Une déclaration d'intention adressée à un groupe de personnes, par exemple les collaborateurs d'un service dans un hôpital, ne constitue pas selon nous une attribution d'autorisation juridiquement valable puisque ce groupe ne possède aucune personnalité juridique en soi.

Dans ce sens, nous aurions attendu que l'autorisation de groupes soit consignée dans l'ordonnance de sorte qu'il s'agisse en principe d'une attribution d'autorisation à des personnes individuelles. Celles-ci seraient ensuite représentées en tant que groupe dans les différents registres de la communauté ou communauté de référence. Mais le projet d'ordonnance va exactement dans la direction opposée. Il établit expressément que les patients peuvent accorder des autorisations à des groupes de professionnels de la santé. La composition de ces groupes doit simplement être claire à tout moment.

L'OFSP est manifestement conscient que cette approche peut devenir problématique. Car d'une part, les communautés doivent s'assurer que les groupes ne sont pas démesurés et, d'autre part, le commentaire sur les conditions techniques et organisationnelles de certification souligne qu'il ne faut pas accorder d'autorisation à un nombre disproportionné de professionnels de la santé hors contexte thérapeutique. La disposition établissant que les groupes ne doivent pas être trop importants nous paraît peu appropriée. Personne ne pourra définir ici une échelle de la taille du groupe pour l'évaluation de la proportionnalité. Une règle pourrait en principe être trouvée avec le contexte thérapeutique, mais l'ordonnance et la remarque susmentionnée la vident totalement de sens. Une autorisation qui ne serait pas

délivrée expressément par le patient à des professionnels de la santé extérieurs au contexte thérapeutiques devrait être totalement exclue.

L'un des principes définis pour eHealth Suisse énonce que seuls les professionnels de la santé participant au traitement doivent avoir accès au dossier électronique du patient. L'indication de l'OFSP selon lequel le nombre de professionnels de la santé disposant d'un droit d'accès alors qu'ils ne participent pas au traitement ne devant pas être important n'est pas compréhensible. En outre, cette problématique est accentuée par le fait qu'il peut s'agir d'un groupe fluctuant. On peut donc supposer qu'un professionnel de la santé entrant dans le groupe obtiendra automatiquement les autorisations d'accès correspondantes. Dès lors, on ne peut plus parler d'une attribution d'autorisation par le patient.

Il convient également de prêter une attention particulière au rôle des assistants des professionnels de la santé. Ces personnes doivent également avoir accès au dossier électronique du patient, bien que cela ne soit mentionné ni dans la loi, ni dans le projet d'ordonnance. Le cercle des détenteurs de l'autorisation d'accès s'élargit donc encore. Par conséquent, les données du protocole doivent permettre aux patients de savoir quels assistants accèdent à leur dossier électronique et pour quels professionnels de la santé ils travaillent. Car au final, c'est bien le professionnel de la santé qui est responsable de ses assistants.

D'une manière générale, l'analyse des dispositions d'exécution relatives à la LDEP nous a donné l'impression qu'on ne visait plus clairement une séparation stricte des systèmes primaires (p. ex. système d'information sur les patients d'un hôpital ou d'un cabinet) et secondaires (p. ex. service de consultation de la communauté). Ce qui montre peut-être déjà que le dossier électronique du patient évoluera vers une sorte de système primaire.

1.5.2 Etablissement des faits auprès du service médical de la Confédération

L'établissement des faits effectué auprès du service médical de l'administration fédérale et des entreprises de la Confédération (MedicalService AeD) a permis d'établir que ce dernier respectait les exigences en matière de protection des données. La procédure a été close.

Dans le cadre de nos activités de surveillance, nous avons engagé une procédure d'établissement des faits à l'automne 2014 auprès du service médical de la Confédération. À la demande de plusieurs citoyens, nous avons donc examiné à cette occasion le traitement de données concernant la santé dans le domaine du travail (cf. notre [22^e Rapport d'activités](#) 2014/2015, chiffre 1.5.4).

Nous avons tout d'abord examiné les processus et les traitements de données sur la base des documents fournis par le service médical et, en janvier 2015, avons procédé à un contrôle sur place. Le service médical n'informe l'administration fédérale que sur les «conclusions des constats médicaux» et ne communique aucun diagnostic ou résultat tiré de ses examens médicaux concernant l'aptitude des candidats pour raison de santé.

Cet établissement des faits a montré que l'organisation et les traitements de données du service médical remplissaient les conditions définies par la loi sur le personnel de la Confédération et les exigences figurant dans la loi sur la protection des données. Sur la base de ces résultats, nous avons clos notre contrôle.

1.5.3 Refus de renseignements sur les données de santé d'un enfant

Durant l'exercice sous revue, il nous a été demandé si une caisse-maladie pouvait refuser, en cas de garde partagée, de fournir à un parent les données sur la santé d'un enfant incapable de discernement lorsque cet enfant se trouve sous la garde de l'autre parent après un divorce ou une séparation.

Conformément à l'article 8 de la loi fédérale sur la protection des données (LPD), le représentant légal peut exercer le droit d'accès à la place de la personne mineure et incapable de discernement. En principe, les représentants légaux sont les parents. Indépendamment de la personne qui a la garde de l'enfant dans une garde partagée, les deux parents peuvent faire valoir ce droit d'accès, qui doit leur être accordé à tous les deux.

La situation est tout autre dans les cas où certaines informations ne peuvent plus être confiées à l'un des parents afin de protéger l'enfant. Cependant, ce n'est pas à la caisse-maladie d'évaluer de tels cas conflictuels. De même, elle ne peut s'appuyer sur les seules directives de l'un des parents. En cas de litige, elle doit s'en tenir à la décision officielle d'un tribunal ou de l'autorité de protection de l'enfant et de l'adulte (APEA).

1.6 Assurances

1.6.1 Contrôle des services de réception de données des assureurs-maladie

Comme mentionné dans le rapport d'activités 2014/2015, chaque assureur-maladie doit disposer, depuis le 1^{er} janvier 2014, d'un service de réception des données (SRD) certifié pour la réception des factures de type «Diagnosis Related Groups» (DRG). Les contrôles que nous avons effectués cette année ont montré que la mise en œuvre de ces SRD fonctionnait bien. Dans quelques cas, nous avons constaté des lacunes que nous avons notifiées au service de certification concerné.

Durant l'année sous revue, nous avons contrôlé sept SRD certifiés dans le cadre de procédures d'établissement des faits. Des interfaces avec divers autres acteurs ont également été examinées à cette occasion (p. ex. l'interface entre intermédiaires et SRD).

Lors de ces contrôles, nous avons généralement constaté les mêmes problèmes que l'année dernière. C'est pourquoi nous renvoyons ici aux commentaires du [22^e rapport d'activités](#) (chiffre 1.6.1).

Durant l'exercice sous revue, plusieurs séances ont été à nouveau organisées avec l'Office fédéral de la santé publique (OFSP) afin de coordonner les activités de surveillance des deux autorités qui peuvent se recouper, et d'aborder des questions en suspens concernant les SRD ainsi que d'autres thèmes liés.

Par ailleurs, deux séances ont eu lieu avec les certificateurs des SRD et avec le service d'accréditation (SAS). Cette année encore, ces réunions ont permis des discussions concernant la certification, la mise en œuvre et la fonction des SRD, les interfaces entre les différents acteurs (hôpitaux, intermédiaires, etc.) et la clarification de certaines divergences d'opinion.

Avec le recul, nous pouvons constater que la mise en œuvre de l'article 59a de l'ordonnance sur l'assurance-maladie (OAMal) se déroule toujours de manière fructueuse et globalement conforme à la loi. La collaboration avec les certificateurs, les assureurs et les exploitants de SRD électroniques a été constructive.

1.6.2 Facturation dans le domaine SwissDRG – que peut-on transmettre au médecin-conseil?

Dans le cadre de la facturation dans le domaine SwissDRG, des informations de santé très détaillées parviennent à l'assurance-maladie avec la facture et le jeu de données dans un format défini (Minimal Clinical Dataset, MCD). Il se pose dès lors la question de savoir si ces informations font également partie des données médicales qui peuvent être transmises au médecin-conseil.

Depuis le 1^{er} janvier 2012, les prestations d'hospitalisation au sein des hôpitaux et maternités sont rémunérées par des forfaits par cas reposant sur le diagnostic (SwissDRG). Les prestataires doivent parallèlement transmettre le Minimal Clinical Dataset (MCD) avec la facture au service de réception des données de l'assurance-maladie. Le MCD contient le diagnostic principal, les éventuels diagnostics secondaires et les procédures sous forme codée. Les informations qu'il contient doivent être clairement désignées comme des données médicales. Outre des informations administratives sur le prestataire et le patient, la facture (invoice) contient également des chiffres tarifaires. Selon nous, ceux-ci constituent des données médicales. Cela vaut en particulier pour le code DRG, qui, s'il est un chiffre, fournit des indications claires sur l'état de santé du patient.

Le catalogue de forfaits par cas DRG est différencié au point que la majorité des codes DRG correspondent assez précisément au diagnostic concret. C'est pourquoi nous avons examiné en détail, pendant l'année sous revue, les cas où le patient exigeait la transmission de toutes les données médicales au médecin-conseil, ou dans lesquels le prestataire s'en chargeait lorsque cela se justifiait sur la base de la disposition correspondante de la loi fédérale sur l'assurance-maladie (LAMal). Nous avons examiné en particulier la question de savoir si la facture avec le code DRG devait être transmise par le service de réception des données au médecin-conseil et non au service des prestations. Il y a lieu de constater ici que le format prescrit par le «Forum Datenaustausch» (XML 4.4) n'autorise actuellement aucun marquage de la facture (invoice) comme «destinée au médecin-conseil» (marquage «confidentiel»). Seul le MCD peut être marqué ainsi par le prestataire. Mais le format (XML 4.4) ne satisfaisant de toute façon pas aux dispositions légales, on ne peut en déduire que la facture ne peut pas être adressée également au médecin-conseil.

Comme nous l'avons établi dans nos clarifications, de nombreux prestataires marquent tous les MCD comme destinés au médecin-conseil. On ne peut toutefois supposer que les conditions légales autorisant un transfert du MCD au médecin-conseil ont toujours été respectées dans ces hôpitaux. Un nombre également

élevé d'hôpitaux ne marquent jamais le MCD comme étant destiné au médecin-conseil. Là encore, on ne peut supposer qu'aucun patient n'a demandé la transmission des données au médecin-conseil dans ces hôpitaux. Par ailleurs, nous avons l'impression qu'une partie des hôpitaux n'emploie pas la marque «confidentiel» au sens de la loi. Il est très probable que trop de MCD parviennent ainsi au médecin-conseil, mais pas tous ceux qui le devraient.

Sur la base des incertitudes constatées, nous avons également contacté l'Office fédéral de la santé publique (OFSP) afin de connaître la procédure correcte à appliquer concernant la facture. Selon l'OFSP, le code DRG est principalement un chiffre de prestation destiné à l'assureur (service des prestations), même s'il contient également, dans une certaine mesure, des données relatives à la santé. Sur la base d'une analyse approfondie des dispositions légales déterminantes et d'autres clarifications, nous avons été amenés à notifier les faits au chef du Département fédéral de l'intérieur (DFI), notamment au regard de la prochaine extension des forfaits par cas et donc du décompte par facture du type SwissDRG aux domaines de la rééducation et de la psychiatrie hospitalières. Les incertitudes actuelles devraient être clarifiées par le législateur avant cette extension. La situation actuelle n'est pas satisfaisante du point de vue de la protection des données et des droits du patient. Cela n'a pas de sens que le patient ou le prestataire puisse faire transmettre les données médicales au médecin-conseil lorsque le service des prestations de l'assureur est informé de l'état de santé du patient dans la facture.

La demande que nous formulons est donc claire: il convient de s'assurer, dans le développement du format des factures du type SwissDRG, que la facture puisse également être marquée «confidentiel». De même, les dispositions pertinentes de la LAMal et de l'ordonnance connexe doivent être précisées. Le contenu de la facture doit notamment être défini plus en détail. Les assureurs-maladie devraient obtenir les informations nécessaires au contrôle des factures sans léser le droit des patients à la transmission des données médicales au médecin-conseil. Par ailleurs, il convient de s'assurer par une information appropriée que le fournisseur de prestation utilise correctement le marquage «confidentiel» afin d'éviter de surcharger inutilement les médecins-conseils de l'assureur-maladie. Le DFI a manifestement reconnu le problème et nous a donc assuré que nos réflexions seraient intégrées dans la nouvelle législation.

1.6.3 Suppression des données auprès des assurances-accidents

De nombreux citoyens nous ont contactés pour nous signaler qu'ils n'étaient pas d'accord que des assureurs-accidents stockent des données les concernant pendant des décennies. La démarche des assureurs est cependant correcte.

Durant l'année sous revue, nous avons souvent été contactés via notre ligne de conseil téléphonique par des citoyens qui avaient soumis une demande de suppression de données à une assurance-accident (assureur-accident obligatoire au sens de la loi fédérale sur l'assurance-accidents, LAA). Ils faisaient valoir qu'il s'agissait souvent d'accident-bagatelle et que les informations étaient déjà très anciennes (20 ans, voire davantage).

Il convient ici de noter que la loi ne fixe aucun délai maximal de conservation pour l'assurance-accidents. Cela tient à la nécessité d'établir un lien de causalité adéquat entre le sinistre et le dommage survenu, qui est déterminant pour l'obligation de prestation de l'assureur. En cas de sinistre, celui-ci étudiera si le dommage survenu a bien été provoqué par l'accident selon un lien de causalité adéquat. Il vérifiera en particulier si la personne assurée ne subissait pas des dommages antérieurs ou des symptômes de maladie qui auraient pu contribuer, voire causer le dommage survenu. C'est pourquoi l'assureur doit pouvoir accéder à des informations, même anciennes, en cas de sinistre. En ce sens, la durée de conservation très longue n'enfreint donc pas le principe de proportionnalité. Naturellement, un assureur-accidents peut décider lui-même de ne plus conserver, et donc de supprimer ou de détruire des informations qui ont atteint une certaine ancienneté. Mais il n'existe pas pour autant de prétention générale à la suppression.

1.6.4 Ordonnance sur la surveillance de l'assurance-maladie sociale – projet BAGSAN

Pour la surveillance des assureurs-maladie sociaux, l'Office fédéral de la santé publique exige de ces établissements des indications très détaillées sur chaque personne assurée. Nous nous sommes exprimés à ce sujet dans le cadre de la consultation des offices concernant l'ordonnance sur la surveillance de l'assurance-maladie sociale. Les dispositions légales actuellement en vigueur sont insatisfaisantes.

Le 1^{er} janvier 2016 est entrée en vigueur la nouvelle loi concernant la surveillance de l'assurance-maladie (LSAMal). Une consultation des offices a été menée durant l'exercice sous revue pour les dispositions d'exécution à intégrer dans l'ordonnance

connexe (OSAMal). Du point de vue de la protection des données, les dispositions relatives à la transmission à l'Office fédéral de la santé publique (OFSP) par les assureurs-maladie de données individuelles sur chaque personne assurée étaient particulièrement importantes. L'OFSP souhaiterait utiliser ces données individuelles pour assumer ses nouvelles fonctions de surveillance ou de mises en œuvre. C'est dans ce contexte que figure également le projet BAGSAN, projet statistique visant à appliquer la stratégie «Santé 2020» du Conseil fédéral. Celui-ci doit jeter les bases d'un pilotage plus efficace du système de santé.

Dans le cadre de la consultation des offices, nous nous sommes intéressés de près aux données individuelles à livrer et notamment au processus de transmission à l'OFSP. Sur la base de cette analyse, nous avons fait remarquer à l'OFSP que le processus de transmission prévu était en contradiction avec l'obligation des assureurs-maladie de garantir l'anonymat des assurés. Ce processus entraînerait notamment une transmission de données personnelles pseudonymisées. Selon nous, la préservation de l'anonymat des assurés dans de telles circonstances relève d'abord de la responsabilité de l'Office fédéral destinataire des données et assurant leur traitement ultérieur, en l'occurrence l'OFSP. Cette conclusion découle également du fait que l'office devrait obtenir le droit de coupler les données évoquées ici avec des informations provenant d'autres sources. Par ailleurs, nous avons également souligné à l'OFSP qu'une partie des données à transmettre devaient être considérées comme des données personnelles sensibles et que les assureurs-maladie, en tant qu'organes fédéraux opérant dans le domaine de l'assurance obligatoire, avaient besoin d'une base légale ancrée dans une loi fédérale pour transmettre ces données à l'OFSP.

Comme nous l'avons ensuite constaté lors d'une deuxième consultation des offices, les dispositions concernant la transmission de données d'assurés ont été supprimées de l'OSAMal. En revanche, l'ordonnance sur l'assurance-maladie (OAMal) a été adaptée de sorte que les données de surveillance que les assureurs doivent livrer conformément à cette ordonnance puissent également être utilisées aux fins de la LSAMal. Cette démarche nous semble problématique pour deux raisons. La première relève de la technique législative. Une partie des dispositions d'exécution de la LSAMal se trouvent non pas dans l'OSAMal qui s'y rapporte, mais dans l'OAMal, ce qui risque d'entraîner des confusions. La seconde est liée à l'importance très contestée des dispositions actuelles de l'OAMal, qui reposent pour l'heure sur une disposition très ambiguë de la LAMal. C'est pourquoi le législateur doit, à la prochaine occasion, préciser ces dispositions et les adopter au niveau normatif approprié. Nous avons communiqué cette conclusion à l'OFSP dans le cadre de

notre activité de conseil. Jusqu'à l'approbation de nouvelles dispositions, les assureurs-maladie doivent respecter les dispositions en vigueur de l'OAMal et garantir l'anonymat des assurés lors de la transmission de données à l'OFSP.

1.6.5 Ordonnance sur la compensation des risques dans l'assurance-maladie

L'amélioration de la compensation des risques doit décharger davantage les assurances-maladie affichant une mauvaise structure de risque. Pour cela, les assureurs-maladie doivent fournir à l'Institution commune LAMal de nouvelles livraisons de données individuelles, avec des indications sur les médicaments utilisés.

Dans le cadre de la consultation des offices, nous nous sommes exprimés sur la révision de l'ordonnance sur la compensation des risques dans l'assurance-maladie. Cette révision vise à affiner la compensation des risques et donc à décharger davantage les assureurs-maladie affichant une mauvaise structure de risque. Afin de calculer la compensation des risques, les assureurs-maladie fournissent à l'Institution commune LAMal les données qui permettent de regrouper les assurés selon plusieurs indicateurs de risque. De nouveaux indicateurs doivent être introduits en complément des indicateurs actuels de l'âge, du sexe et du séjour dans un hôpital ou un EMS. Il s'agit en l'occurrence de l'indicateur des groupes de coûts pharmaceutiques (PCG), formé à partir de données issues du secteur ambulatoire, ainsi que de celui du coût des médicaments. Cela permettra de tenir compte du fait qu'une part considérable des coûts de l'assurance maladie est générée par des traitements médicamenteux très onéreux. Etant donné que des données individuelles sur les différents assurés doivent être fournies pour la première fois, avec des indications sur les médicaments qu'ils utilisent, la transmission des données des assureurs à l'Institution commune LAMal prend une nouvelle dimension du point de vue du droit de la protection des données.

Au moment de la consultation des offices, la mise en œuvre concrète de la livraison des données n'était pas encore claire car l'Institution commune LAMal doit pour cela développer un nouvel outil de collecte de données, et l'ordonnance stipule que la transmission doit être conforme aux instructions de l'Institution commune LAMal. Seules les explications sur le projet d'ordonnance établissaient que les données devaient être fournies sous une forme anonyme. Par ailleurs, les informations à livrer n'étaient pas clairement définies dans l'ordonnance. C'est donc l'Office fédéral de la santé publique qui devait déterminer les règles de transmission des

données et définir clairement les données dans l'ordonnance. Nous avons également constaté qu'il ne s'agissait pas ici d'une transmission de données anonymes, mais de données personnelles pseudonymisées. À notre connaissance, les données à fournir ont ensuite été intégrées dans le projet d'ordonnance conformément à nos remarques, et il a été précisé que les données étaient transmises sous forme pseudonymisée. En revanche, le fait que l'Institution commune LAMal détermine les règles de transmission des données a été maintenu. Néanmoins, elle consultera l'OFSP concernant les instructions, qui devront en outre être approuvées par ce dernier. Ainsi, l'organe fédéral compétent en la matière assumera comme il se doit la responsabilité des modalités de transmission à respecter.

1.7 Secteur du travail

1.7.1 Contrôle de sécurité relatif aux collaborateurs (dans le domaine privé)

Suite à diverses requêtes, nous avons clarifié les exigences en matière de contrôle de sécurité relatif aux personnes dans le domaine privé et rédigé des explications à ce sujet.

Des prestataires de services pour des établissements financiers nous ont demandé dans quelle mesure le droit de la protection des données autorise la transmission de certaines données concernant leurs collaborateurs à leurs mandants, telles que des extraits du casier judiciaire ou du registre des poursuites. Les établissements financiers avaient besoin de ces informations pour s'assurer que la sécurité des données était garantie.

Sur la base de ces requêtes, nous avons étudié cette problématique en profondeur. Pour cela, nous avons rencontré, d'une part des établissements financiers, et d'autre part les autorités de surveillance correspondantes, afin de connaître les différents besoins et les exigences en matière de contrôle des collaborateurs. Les variations du potentiel de risque des collaborateurs ainsi que les dispositions spécifiques qui s'appliquent nous ont ainsi été décrites. Par ailleurs, nos interlocuteurs nous ont indiqué qu'un traitement différencié des collaborateurs internes et externes n'était pas utile.

Nous avons ensuite analysé les faits en tenant compte des dispositions pertinentes du droit de la protection des données et du code des obligations. À cet égard, nous avons accordé une attention particulière au principe de proportionnalité, qui ne peut toutefois être concrètement vérifié qu'en procédant au cas par cas. Nous avons rédigé pour les employeurs privés et les collaborateurs concernés des explications sur les dispositions du droit de la protection des données qui doivent être respectées lors de l'examen des risques. Ces commentaires ont été publiés [sur notre site Internet](#).

1.7.2 Bureau de communication pour lanceurs d’alerte (whistleblowing) de la Confédération

Le Tribunal fédéral ayant décidé de ne pas entrer en matière dans l’affaire du bureau de communication pour lanceurs d’alerte de la Confédération, l’arrêt du Tribunal administratif fédéral est maintenant entré en vigueur.

Comme nous l’avons indiqué dans le [22^e rapport d’activités](#) 2014/2015 (chiffre 1.7.3), le Contrôle fédéral des finances (CDF), qui gère le bureau de communication pour lanceurs d’alerte, a porté le jugement du Tribunal administratif fédéral devant le Tribunal fédéral. Celui-ci a décidé de ne pas entrer en matière par son arrêt du 12 novembre 2015. Pour le motiver, il a indiqué que le CDF ne possédait pas la qualité pour recourir. Le Tribunal fédéral n’est donc pas entré en matière par défaut de légitimation et de respect des obligations de motivation. L’arrêt du Tribunal administratif fédéral du 16 décembre 2014 est donc entré en vigueur et oblige le CDF à nous déclarer ses fichiers et à établir un règlement de traitement.

1.8 Économie et commerce

1.8.1 Safe Harbor: arrêt de la Cour de justice de l'Union européenne et conséquences pour la Suisse

Dans son arrêt du 6 octobre 2015, la Cour de justice de l'Union européenne a invalidé l'accord Safe Harbor de protection des données entre l'Union européenne (UE) et les États-Unis. Elle a constaté que la transmission de données personnelles vers les États-Unis sous le régime de l'accord dit Safe Harbor était problématique. Qu'implique cette décision pour la Suisse?

Dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14 (Schrems), la CJUE a invalidé la décision de la Commission selon laquelle les États-Unis garantissaient un niveau de protection adéquat des données à caractère personnel transmises. Comme la CJUE le constate, il n'existe pour les données transmises aux États-Unis dans le cadre de l'accord Safe Harbor aucune protection suffisante contre des accès disproportionnés des autorités. Elle ajoute qu'il n'existe pas non plus de protection juridique efficace contre de tels accès pour les personnes se trouvant hors des États-Unis.

En 2008, la Suisse a conclu avec les États-Unis un accord comparable et au contenu très similaire: le «U.S.-Swiss Safe Harbor Framework» (ci-après l'accord Safe Harbor Suisse-E.-U.). Nous avons de ce fait analysé la situation actuelle en matière de transmissions de données de la Suisse vers les États-Unis et sommes parvenus à la conclusion que les points faibles mis en lumière par la CJUE s'appliquaient également à l'accord Safe Harbor Suisse-E.-U.

Ce dernier est en effet un système comportant une autocertification pour des entreprises souhaitant transférer des données de la Suisse aux États-Unis. Les garanties de protection des données qu'il contient n'engagent cependant que les entreprises certifiées proprement dites, mais pas les autorités publiques. Il n'existe aucune autre réglementation contractuelle ou nationale limitant les accès des autorités à ces données. En revanche, certaines réglementations nationales permettent d'une manière générale la conservation de données personnelles par les autorités américaines ou leur utilisation, sans différenciation, restriction, exception ou limitation d'accès. Il n'y a donc pas de protection adéquate contre les accès disproportionnés des autorités américaines à des données à caractère personnel transmises de la Suisse aux États-Unis.

En 2008, ce point n'était pas encore une priorité lors de l'examen des garanties requises en vue de l'accord entre la Suisse et les États-Unis. On pouvait à l'époque en toute bonne foi partir du principe que la pratique appliquée par les autorités en

matière de traitement de données personnelles était comparable dans les deux pays, de sorte qu'aucun besoin de réglementation n'avait été identifié. Suite aux révélations d'Edward Snowden, des divergences flagrantes ont été mises à jour dans la conception des deux pays de ce qui doit être autorisé pour la préservation de la sécurité nationale. Il y a donc aujourd'hui pour le moins de sérieux doutes quant à la possibilité de considérer comme proportionnés, selon la conception de la Suisse, les accès des agences américaines de renseignement aux données personnelles de citoyens non américains. Il s'est aussi avéré que les entreprises américaines certifiées donnaient généralement immédiatement suite aux demandes d'accès des autorités américaines, sans respecter les garanties énoncées dans l'accord Safe Harbor Suisse-E.-U.

En outre, les mesures prévues dans cet accord pour assurer la protection juridique des personnes concernées ne sont toujours contraignantes que pour les entreprises certifiées. Il n'existe par contre aucune protection juridique efficace contre des accès des autorités pour des personnes hors des États-Unis. Ces personnes n'ont ainsi aucune possibilité de se défendre, dans le cadre d'une procédure judiciaire, contre le traitement de leurs données par les autorités américaines.

Même si la décision de la CJUE d'invalider l'accord Safe Harbor européen ne concerne pas directement l'accord helvétique, la Suisse ne peut adopter aucune position différenciée sur ce sujet. Si elle s'attachait à son accord sans le modifier, une telle attitude pourrait avoir pour conséquence, outre les risques susmentionnés pour les droits fondamentaux des personnes concernées, que l'UE annule sa déclaration d'adéquation concernant le niveau de protection des données en Suisse. Et ce, notamment parce que le maintien de l'accord initial permettrait de contourner d'éventuels nouveaux accords plus stricts avec les États-Unis grâce à un transfert de données UE-Suisse-États-Unis. Une annulation de la déclaration d'adéquation aurait des conséquences graves pour le libre-échange de données personnelles avec les pays de l'UE et pourrait conduire à l'isolement de la Suisse.

L'autre possibilité, qui consisterait à assurer un niveau de protection adéquat pour l'échange de données avec les États-Unis par des garanties contractuelles (conformément à l'art. 6, al. 2 LPD), n'est pas non plus à même d'empêcher un accès disproportionné des autorités américaines à des données à caractère personnel car un tel contrat entre exportateur et importateur n'est pas contraignant pour les autorités.

La clarification de cette situation ne peut se faire qu'au niveau politique. C'est pourquoi nous avons recommandé au Conseil fédéral de suspendre ou de résilier l'accord Safe Harbor Suisse-E.-U. Celui-ci doit être renégocié afin de remplir les

exigences du droit suisse de la protection des données. Etant donné que seule une démarche commune avec l'UE et ses États membres peut permettre d'atteindre nos objectifs, la Suisse doit coordonner son action avec les autorités compétentes de l'UE.

Le Conseil fédéral a analysé la situation sur la base de nos recommandations et d'interpellations parlementaires allant dans le même sens, et a confirmé le besoin d'action que nous avons soulevé. Il a expliqué qu'il observait la démarche suivie par l'UE et coordonnerait ses mesures avec cette dernière.

L'échange de données avec des entreprises des États-Unis ne pouvant être interrompu jusqu'à la clarification de la situation, les sociétés concernées doivent se couvrir en attendant. À cet égard, il y a lieu de recourir en priorité à des garanties contractuelles complémentaires. Même si, comme indiqué précédemment, ces garanties ne permettent pas de résoudre entièrement le problème des accès disproportionnés des autorités, cette procédure devrait néanmoins améliorer le niveau de protection des données par rapport aux garanties de l'accord Safe Harbor Suisse-E.-U., grâce aux règles supplémentaires suivantes:

Si l'accès à des données personnelles par les autorités américaines ne peut pas être restreint ou empêché, ce problème doit être, du moins partiellement, compensé par des exigences accrues en matière de transparence du traitement des données. Par conséquent, les personnes concernées doivent être informées clairement et de la manière la plus complète possible que leurs données sont transmises aux États-Unis, où les autorités locales peuvent y accéder. Ces personnes doivent être soutenues dans une mesure raisonnable pour faire valoir leurs droits aux États-Unis. Les demandes d'accès des autorités américaines ne doivent pas être satisfaites les yeux fermés: les entreprises doivent réellement exécuter les procédures qui sont à leur disposition pour empêcher de tels accès, et accepter les jugements qui en résultent. Ce faisant, il y a lieu de noter qu'en Suisse les personnes concernées ont à tout moment la possibilité de faire examiner des données devant être transmises aux États-Unis par un tribunal civil. Dans de tels cas, il faut attendre un jugement juridiquement valide avant de transmettre les données.

Des informations complémentaires à ce sujet sont disponibles [sur notre site Internet](#).

1.8.2 Bases légales des compteurs intelligents (smart metering) en Suisse

Dans le cadre de la préparation des bases légales en vue de l'introduction dans toute la Suisse des «compteurs électriques intelligents» (smart meters), nous avons participé à une séance du groupe d'accompagnement de l'Office fédéral de l'énergie (OFEN). Sur la base des résultats obtenus, nous avons conseillé l'Office fédéral dans l'élaboration des dispositions légales.

L'Office fédéral de l'énergie nous a invité à prendre part au groupe d'accompagnement Sécurité et protection des données pour le smart metering, qui a élaboré les bases d'une réglementation uniforme des compteurs intelligents dans toute la Suisse. Nous avons apporté des remarques quant aux exigences du droit de la protection des données, notamment en ce qui concerne la finalité et la conservation des données saisies. L'OFEN a remanié les dispositions légales sur la base de nos remarques et les a intégrées dans les délibérations parlementaires en cours relatives à la Stratégie énergétique 2050 afin de créer les conditions d'introduction d'un smart metering régi de manière uniforme dans toute la Suisse (cf. [22^e rapport d'activités](#) 2014/2015, chiffre 1.8.1 et [21^e rapport d'activités](#) 2013/2014, chiffre 1.8.1).

1.8.3 Carte-client du commerce de détail

Les clauses de consentement figurant dans les conditions générales posent parfois problèmes. L'introduction de l'analyse du panier des achats, liée à la Supercard de la Coop, a entraîné une modification des conditions générales permettant désormais à la Coop de recueillir le consentement de ce même client pour l'analyse de ses données d'achats. Les clients ont eu la possibilité d'accepter les nouvelles conditions générales en cochant la case nécessaire et l'analyse du panier et les paragraphes correspondant des conditions leur ont été à nouveau signalés.

Coop propose sa carte-client Supercard depuis l'année 2000. Aujourd'hui, plus de trois millions de ménages la possèdent. En 2005, nous avons contrôlé le traitement des données effectuées sur la base de cette carte-client et émis plusieurs propositions d'amélioration ainsi que des recommandations dans notre rapport final. L'objet du nouveau contrôle était d'une part la mise en œuvre de nos propositions et recommandations d'alors. D'autre part, nous voulions examiner les principales modifications en rapport avec le programme Supercard sous l'angle du droit de la protection des données.

Notre examen de la situation a montré que Coop avait mis en œuvre toutes les propositions et recommandations figurant dans notre rapport final de 2005. L'analyse

des données d'achats (analyse du panier) introduite en septembre 2012 en vue d'une approche ciblée de la clientèle est la nouveauté la plus importante attachée à la Supercard. À cet effet, Coop a modifié les conditions générales de cette carte. Celles-ci informent de manière transparente sur le genre et le but du traitement des données ainsi que sur les droits des personnes concernées. Par exemple, les «Superboxes» placées dans les filiales Coop ont permis d'attirer l'attention des clients sur les modifications des conditions générales et de leur demander leur consentement. Même sans celui-ci, l'utilisation de la Supercard reste possible sans inconvénient majeur.

Les nouveaux participants au programme Supercard doivent accepter les nouvelles dispositions et, de ce fait, l'analyse du panier d'achats. La transformation du traitement des données en analyse du panier d'achats constituant un grand changement pour la clientèle existante, une modification unilatérale des conditions générales peut être problématique malgré l'acceptation par les clients à la Superbox: certains clients n'étaient pas conscients de la portée du traitement des données ou ont lu les nouvelles conditions en les survolant. La Coop a quelque peu désamorcé le problème en attirant à nouveau l'attention, au moment même du consentement, sur les nouvelles conditions, sur l'analyse du panier d'achats et sur les paragraphes correspondants des conditions générales. L'analyse du panier d'achats n'avait pas été totalement mise en œuvre au moment de notre contrôle. Nous avons toutefois constaté qu'à ce propos, la Coop est consciente du caractère problématique de la question du point de vue de la protection des données et s'efforce de procéder avec soin à la mise en œuvre requise dans les systèmes. À ce sujet, il faut en particulier souligner la transparence de l'information destinée aux clients, que ce soit sur le site Internet de la Supercard ou dans les divers articles parus dans le journal de la Coop. Néanmoins, malgré l'image d'ensemble globalement positive, nous avons formulé dans notre rapport final des propositions d'amélioration quant aux exigences en matière de transparence et quant à la communication des informations. La Coop les a toutes acceptés et assurera la mise en œuvre.

1.8.4 Échanges de contenus sur Internet et droits d'auteur – révision de la loi sur le droit d'auteur

L'exigence d'information en procédure civile prévue par la révision de la loi sur le droit d'auteur, ainsi que la soumission d'avertissements et la procédure «Stay Down» prévue pour certains cas, sont problématiques du point de vue de la protection des données.

La loi fédérale sur le droit d'auteur et les droits voisins (LDA) est en phase de révision. Cette révision doit notamment assurer la mise en œuvre des mesures proposées par le groupe de travail AGUR12 pour améliorer la protection des droits d'auteur sur

Internet (cf. notre [21^e rapport d'activités](#) 2013/2014, chiffre 1.3.1). Quelques-unes de ces mesures soulèvent des questions du point de vue de la protection des données:

Avec la LDA révisée, un droit à l'information doit être introduit dans le cadre de l'action en exécution de droit civil: un titulaire de droit qui souhaite porter plainte contre un contrevenant dont il ne connaît que l'adresse IP (ce qui est p. ex. régulièrement le cas pour les œuvres proposées au téléchargement sur les réseaux peer-to-peer) doit obtenir de l'opérateur Internet le nom de la personne qui détenait l'adresse IP en question au moment des faits.

Cette information doit aujourd'hui être sauvegardée pendant six mois par les opérateurs en raison de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), et elle est protégée par le secret des postes et des télécommunications. Cette obligation de conservation, introduite pour lutter contre des infractions graves, est compliquée sur le plan de l'État de droit: elle représente une atteinte grave aux droits de la personnalité des utilisateurs d'Internet, dont les données sont mémorisées à titre préventif sans justification concrète, ce qui doit en principe être considéré comme un traitement de données disproportionné. Lors de l'introduction de la LSCPT, et dans les débats relatifs à sa révision actuelle [cf. chiffre 1.4.1 du présent rapport d'activité], il a également été régulièrement souligné que seule l'élimination d'infractions graves pouvait justifier cette atteinte. Il a été constamment confirmé que l'utilisation des données stockées devait être limitée aux procédures pénales. De même, la Cour de justice de l'Union européenne (CJUE) exige dans son arrêt du 8 avril 2014 sur la conservation des données que les autorités de poursuites pénales ne puissent obtenir l'accès aux données accessoires qu'à des conditions strictes. Dans ce cadre étroit, le PFPDT a jugé que la conservation des données était justifiée.

Cependant, il est prévu d'utiliser ces données dans le cadre de prétentions de droit civil en relation avec des violations de droits d'auteur et être rendues accessibles aux titulaires de droits. On s'éloigne ainsi nettement du but initial de la conservation des données. D'une part les déclarations faites lors de son introduction sont contredites, et d'autre part, on quitte le cadre étroit fixé par la CJUE dans l'arrêt susmentionné. Etant donné qu'un privilège en faveur de prétentions relatives au droit d'auteur par rapport à d'autres prétentions de droit civil se justifierait difficilement de manière objective, on peut par ailleurs supposer que de telles données seraient accessibles à plus ou moins long terme dans toutes les procédures de droit civil de ce type.

La conservation des données entraînant une atteinte grave aux droits de la personnalité de tous les utilisateurs d'Internet, nous défendons clairement la position

selon laquelle la violation du secret des postes et des télécommunications qui en résulte ne peut se justifier par l'application de prétentions de droit civil. Une telle disposition irait à l'encontre des principes de proportionnalité et de finalité.

Nous mettons sur le même plan la mesure, également prévue, selon laquelle les fournisseurs d'accès à Internet devront soumettre des avertissements à leurs clients si des atteintes aux droits d'auteur sont commises à partir de leur connexion et si les ayants droit l'exigent.

Désormais, les fournisseurs d'hébergement doivent en outre être obligés de supprimer les contenus en infraction avec les droits d'auteur, ce qui ne pose pas de problème au regard du droit de la protection des données, mais ils doivent également s'assurer dans certains cas que ces contenus ne seront pas remis en ligne. À notre connaissance, une telle procédure de «Stay Down» n'est applicable de manière efficace qu'au travers d'une surveillance des utilisateurs, ce qui constituerait une atteinte encore plus grave aux droits de la personnalité des personnes concernées que l'exigence d'information des ayants droits. Les intérêts poursuivis pèsent trop peu, en comparaison, pour justifier une telle violation de ces droits. C'est pourquoi nous jugeons cette mesure disproportionnée. Par ailleurs, cette surveillance serait effectuée à la demande de privés et par des privés (les fournisseurs d'hébergement), de sorte qu'elle serait également problématique sur le plan de l'État de droit.

Pour ces raisons, nous nous sommes exprimés contre cette mesure dans la procédure de révision en cours.

1.8.5 Éclaircissements dans le domaine des agences de renseignement économique et de renseignement en matière de crédit: Moneyhouse

Nous avons déposé une plainte auprès du Tribunal administratif fédéral contre l'agence de renseignements Moneyhouse, car celle-ci n'a pas accepté toutes nos recommandations, Nous attendons notamment une clarification du concept de profil de la personnalité et espérons qu'un arrêt sera rendu cette année encore.

Dans nos deux derniers rapports d'activités, nous avons rendu compte de l'établissement des faits et présenté nos recommandations concernant la plate-forme www.moneyhouse.ch opérée par itonex AG (cf. [22^e rapport d'activités](#) 2014/2015, chiffre 1.8.3). Itonex AG a par ailleurs changé la raison sociale de l'entreprise en Moneyhouse AG (ci-après Moneyhouse) pendant l'année sous revue. L'entreprise n'ayant pas accepté certaines recommandations, nous avons soumis les questions litigieuses à l'appréciation du Tribunal administratif fédéral.

Le contenu de notre plainte concerne en particulier les points suivants:

- Moneyhouse publie des informations personnelles provenant de son propre fichier et les couple à des données d'autres prestataires. Nous estimons que l'élaboration de ses propres données représente déjà des profils de la personnalité, d'autant plus que Moneyhouse permet aux utilisateurs de la plate-forme de constituer des profils encore plus complets. Ce traitement constitue une violation de la personnalité des personnes concernées, qui ne peut être justifiée que par l'obtention de leur consentement. Le dépôt de cette plainte a pour objectif de faire en sorte que Moneyhouse adapte les services proposés de manière à ne plus traiter de profils de la personnalité ou à ce que toutes les personnes dont les profils de la personnalité sont traités par Moneyhouse ou par des utilisateurs de la plate-forme donnent leur autorisation.
- L'indexation par Moneyhouse de tous les contenus de fichiers auprès des moteurs de recherche enfreint le principe de proportionnalité. Nous demandons donc à l'entreprise d'adapter la possibilité de recherche des personnes inscrites au registre du commerce conformément à la pratique adoptée actuellement par l'Office fédéral du registre du commerce sur le site Internet www.zefix.ch.
- Moneyhouse ne communiquant que les informations provenant de son propre fichier, nous souhaitons que l'entreprise transfère les demandes de renseignements reçues aux partenaires de la plate-forme. Il sera ainsi plus facile aux personnes concernées d'exercer leurs autres droits, par exemple pour faire rectifier ou supprimer leurs données.
- Enfin, Moneyhouse doit améliorer la qualité des données en vérifiant davantage leur exactitude. Dans le domaine des questions concernant la solvabilité, Moneyhouse doit contrôler plus systématiquement si les clients peuvent effectivement présenter une justification de leur intérêt, c'est-à-dire si la demande du client à la plate-forme concernant la solvabilité d'une personne est réalisée dans le cadre de négociations contractuelles.

Nous espérons que le Tribunal administratif fédéral rendra sa décision dans le courant de l'année et attendons avec cet arrêt une clarification de la situation juridique, notamment concernant l'interprétation du concept de profil de la personnalité.

1.8.6 Mise en œuvre des droits d'accès et des droits d'opposition à propos d'un vendeur d'adresses - Procédure devant le Tribunal administratif fédéral

Dans notre dernier rapport d'activités, nous avons émis une recommandation à l'intention d'un commerçant d'adresses qui n'avait pas répondu aux demandes d'accès et d'effacement déposées par plusieurs personnes (cf. notre [22^e Rapport d'activités](#) 2014/2015, chiffre 1.8.4). L'entreprise en question n'a pas réagi à notre recommandation et n'a donc pas mis en œuvre les directives que contenait cette recommandation. D'autres personnes s'étant plaintes à nous pour les mêmes motifs, nous avons soumis l'affaire à l'appréciation du Tribunal administratif fédéral en été 2015. La procédure est toujours pendante.

Nous avons souligné à l'attention des personnes concernées qu'elles peuvent intenter une action civile afin de faire valoir leurs droits d'accès et d'opposition conformément à la loi sur la protection des données.

1.8.7 Appels publicitaires illicites à partir d'un centre d'appels

Au cours de l'exercice écoulé, plusieurs personnes se sont plaintes chez nous de recevoir des appels publicitaires indésirables en provenance d'un centre d'appels. Ce centre prétendait procéder à un sondage sur mandat de la protection suisse des données. Mais le but véritable de l'appel était de vendre une offre de blocage de publicité. Ces appels ont également touché des personnes ayant fait inscrire un astérisque à côté de leur numéro de téléphone dans l'annuaire.

Nous avons sommé l'entreprise en question de cesser immédiatement de procéder à des appels publicitaires ou à des sondages en se réclamant de nos services et de respecter l'apposition des astérisques dans l'annuaire. Le procédé décrit enfreignant la loi fédérale contre la concurrence déloyale (LCD), nous avons en outre signalé le cas au Secrétariat d'État à l'économie.

1.9 Finances

1.9.1 Traitement de données client chez Postfinance

L'intégration d'instruments financiers supplémentaires dans une plateforme d'e-banking constitue, selon les circonstances, une modification de la finalité du traitement des données. Une telle modification nécessite le consentement des clients. Postfinance a accepté plusieurs améliorations permettant d'offrir un choix aux clients à la suite de notre procédure d'établissement des faits.

Au cours de l'année écoulée, Postfinance a remanié sa plateforme d'e-banking et a modifié ses conditions générales. Il y est désormais précisé qu'«e-cockpit», un instrument qui, d'une manière générale, attribue automatiquement chaque transaction de client à une catégorie de données déterminée, est obligatoirement intégré à l'interface e-banking. En outre, un outil doit être introduit qui présente au client, en fonction de ses transactions, des offres publicitaires de tiers. Les clients auraient avoir la possibilité de se désinscrire ultérieurement (opting out) de ces offres publicitaires de tiers, mais pas d'e-cockpit.

Une fois connectés sur le portail, les clients de Postfinance sont priés d'accepter les nouvelles dispositions pour pouvoir continuer à accéder à l'e-banking. Nous avons étudié le traitement des données en relation avec ces nouveautés, dans le cadre d'une procédure d'établissement des faits. En parallèle, nous avons demandé à Postfinance de continuer à octroyer à ses clients l'accès à e-finance également après l'entrée en vigueur des nouvelles conditions générales – au moins pendant ladite procédure – même si les clients n'acceptent pas les nouvelles conditions. Les entretiens qui ont suivi avec Postfinance ont montré que ces mêmes clients reçoivent déjà sur la page intermédiaire, après être entrés dans la plateforme d'e-banking, une option leur permettant de se désinscrire des offres publicitaires de tiers.

Nous avons poursuivi les discussions avec Postfinance et sommes parvenus à deux autres améliorations essentielles au début du mois d'avril 2015: les clients peuvent désormais désactiver le traitement de données dans e-cockpit et effacer les données déjà catégorisées. En ce qui concerne les offres publicitaires de tiers, Postfinance demandera à nouveau le consentement des clients qui ont déjà donné leur accord aux nouvelles dispositions de participation avant l'introduction des nouvelles possibilités de choix.

Dans le rapport final, nous avons relevé que Postfinance remplit ses obligations en matière de protection des données grâce à ces améliorations. Il est en particulier

garanti que les clients peuvent se désinscrire des offres publicitaires sans devoir redouter de perdre l'accès électronique à leurs comptes. Nous contrôlerons la mise en œuvre de ces mesures ultérieurement dans le cadre d'un suivi.

1.9.2 Communication de données personnelles à des autorités fiscales étrangères

La Suisse met en œuvre les nouveaux standards dans la lutte mondiale contre la fraude et la soustraction d'impôts. Afin de créer les bases légales nécessaires jusqu'en 2017, le processus législatif fonctionne à plein régime. Il s'agit pour la Confédération de préserver ses intérêts politiques et économiques face aux enjeux internationaux, sans négliger les droits de la personnalité des contribuables. Nous nous sommes engagés à le rappeler à tous les stades de la procédure législative.

a. Convention de l'OCDE et du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale

Lors de l'année sous revue nous avons été sollicités dans le cadre de diverses procédures de consultations relatives à la coopération internationale en matière fiscale. La situation a beaucoup changé depuis que la Suisse s'est engagée en mars 2009 à adhérer aux normes internationales dans ce domaine (cf. [19^e rapport d'activités](#) 2011/2012, chiffre 1.9.1). Le 15 octobre 2013, la Confédération a signé la Convention de l'OCDE et du Conseil de l'Europe concernant l'assistance administrative mutuelle en matière fiscale (Convention). Celle-ci date de 1988 et constitue un instrument de coopération multilatérale permettant aux parties de s'accorder une assistance administrative pour un grand nombre d'impôts.

Plusieurs formes de collaboration sont prévues, y compris l'échange automatique de renseignements. La mise en œuvre en droit interne de ce type d'assistance d'un genre nouveau nécessite la création de bases légales et la révision de certaines normes. Partant, le Conseil fédéral a proposé d'effectuer des aiguillages ponctuels dans la loi fédérale sur l'assistance administrative en matière fiscale (LAAF) afin de l'adapter en conséquence. De surcroît, un projet de loi spéciale a été mis sur pied pour réaliser la réglementation de détail de l'échange automatique de renseignements (voir ci-dessous «b. Échange automatique international de renseignements fiscaux»).

Suite à sa signature, la Convention a fait l'objet d'un projet d'arrêté fédéral portant sur son approbation. La révision partielle de la LAAF est prévue à l'annexe dudit arrêté et a été le sujet principal de nos remarques. Par conséquent, nous avons, en procédure de consultation, particulièrement attiré l'attention du Département

fédéral des finances (DFF) sur des questions relatives à la densité normative, aux droits procéduraux des contribuables et aux problèmes liés à l'utilisation du numéro AVS en tant qu'identificateur fiscal international. Le DFF a partiellement tenu compte de nos remarques, notamment en ce qui concerne la création d'un numéro d'identification sectoriel au lieu d'utiliser le numéro AVS.

Certaines divergences avec le DFF ont subsisté à l'issue de la consultation et ont fait l'objet d'une procédure de co-rapport de notre part auprès du Conseil fédéral. En effet, le projet de modification de la LAAF prévoit par exemple la possibilité de transmettre des données personnelles à d'autres autorités suisses que les autorités fiscales et à des finalités non fiscales. Ceci est problématique à la lumière du principe de spécialité et du respect de la finalité du traitement qui en l'occurrence devrait être strictement fiscal. Dès lors, nous avons proposé de préciser à quelles autorités, autres que fiscales, des données personnelles pourraient le cas échéant être transmises. Dans un tel cas de figure, les droits procéduraux et en particulier le droit d'être entendu des personnes concernées doivent être expressément garantis. Lors des délibérations du 5 juin 2015, le Conseil fédéral a toutefois décidé d'adopter la proposition du DFF sans modifications.

b. Échange automatique international de renseignements fiscaux

Dans notre dernier rapport d'activités (cf. [22^e rapport d'activités](#) 2014/2015, chiffre 1.9.2) nous avons mentionné le groupe de travail mis sur pied suite à l'adoption par l'OCDE en juillet 2014 de la norme concernant l'échange automatique de renseignements en matière fiscale (Common Reporting Standard; CRS ou Standard). Comme précisé, nous avons été entendus concernant divers points en relation avec la protection des données. Les thèmes sensibles ont par conséquent pu être anticipés et discutés. Cette démarche était bienvenue vu l'ampleur considérable du dossier et son calendrier composé de délais pour le moins ambitieux.

Effectivement, dans le courant de l'année 2015 un nombre considérable d'actes législatifs ont été mis en consultation afin de mettre en œuvre le nouveau standard et de respecter les délais imposés par l'OCDE.

Le CRS prévoit que les États échangent automatiquement des renseignements (EAR) sur des contribuables qui détiennent des comptes financiers auprès d'un établissement à l'étranger. Le standard contient en son sein également l'instrument de droit international public obligatoire à la mise en œuvre multilatérale de l'échange automatique. Il s'agit de l'Accord entre autorités compétentes concernant l'échange automatique de renseignements relatifs aux comptes financiers (Multilateral Competent Authority Agreement; MCAA) que la Suisse a signé le 19 novembre 2014. Or, pour être applicables, les dispositions de cet accord ainsi que

celles du CRS doivent être accompagnées d'une loi fédérale d'exécution. Celle-ci sera la nouvelle loi sur l'échange international automatique de renseignements en matière fiscale (LEAR) dont l'entrée en vigueur est prévue pour 2017. Elle contiendra des dispositions relatives à l'organisation, la procédure, les voies de droit ainsi que des dispositions pénales.

Lors de la procédure de consultation nous avons essentiellement plaidé en faveur d'un niveau plus élevé de la densité normative, c'est-à-dire pour une formulation plus claire est détaillée de certaines dispositions. De surcroît, nous avons requis que les contribuables concernés par une déclaration automatique soient expressément informés. Ceci garantit que le principe de transparence et la bonne foi lors des traitements soient honorés. Ces principes présupposent que la personne concernée puisse vérifier préalablement que les informations qui seront transmises à l'étranger ne sont pas erronées. Sans ce mécanisme, le contribuable devrait systématiquement effectuer une demande de droit d'accès auprès d'un institut financier. Une information générale et abstraite par exemple par le biais des conditions générales n'est pas suffisante.

À l'instar de la consultation relative à l'arrêté fédéral portant approbation de la Convention, des divergences ont subsisté en relation avec le projet de LEAR. Le DFF ne les a toutefois pas présentées au Conseil fédéral. Nous les lui avons par conséquent soumises dans la procédure de co-rapport. Dans ce cadre, nous avons, entre autres, réitéré notre position selon laquelle les personnes concernées par une déclaration devraient être informées de manière individuelle et concrète. Lors de ses délibérations du 5 juin 2015, le Conseil fédéral a toutefois décidé d'adopter la proposition du DFF sans modifications.

À l'occasion de la procédure parlementaire, la question de l'utilisation du numéro AVS en tant qu'identificateur fiscal a ressurgi, malgré la décision du Conseil fédéral de créer un numéro sectoriel. Lors de la session d'automne, le Conseil national, désigné comme conseil prioritaire, s'était dans un premier temps rallié à notre position (voir à ce sujet l'avis de droit de l'Office fédéral de la justice du 5 août 2015, publié sur: www.parlament.ch). Toutefois, le Conseil des États a pour sa part opté pour l'utilisation du numéro AVS. Cette divergence s'est finalement soldée, lors du vote final à la session d'hiver, par l'adhésion à la décision initiale du Conseil des États. C'est-à-dire en faveur de l'utilisation du numéro AVS en tant qu'identificateur fiscal international dans le cadre des échanges automatiques de renseignements.

c. Procédure de mise en œuvre de l'EAR entre États

L'exécution du Standard entre États peut se faire de deux manières: soit par le biais d'un accord bilatéral, tel que l'accord signé le 27 mai 2015 entre la Suisse et l'Union européenne (voir ci-dessous «e. Arrêté fédéral sur l'approbation d'un

protocole d'amendement de l'accord sur la fiscalité de l'épargne entre la Suisse et l'UE»), soit sur la base du MCAA, qui se fonde lui-même sur la Convention. Cette seconde solution a été retenue notamment pour l'introduction de l'EAR entre la Suisse et l'Australie (voir ci-dessous «d. Arrêté fédéral concernant l'introduction de l'EAR avec l'Australie»). Une activation sur la base du MCAA doit réunir les quatre conditions suivantes:

- la Convention doit être en vigueur à l'égard des deux États;
- les deux États doivent avoir signé le MCAA;
- les deux États doivent avoir confirmé qu'ils disposent des lois nécessaires à la mise en œuvre du Standard;
- les deux États doivent avoir annoncé au Secrétariat de l'Organe de coordination qu'ils souhaitent appliquer entre eux l'EAR.

De manière plus générale, le choix des États partenaires de la Suisse s'oriente en fonction d'autres critères. Notamment, l'existence de relations économiques et politiques, d'une procédure de régularisation du passé permettant aux contribuables, si nécessaire, d'arranger leur situation fiscale, d'un accès au marché et d'un niveau de protection des données suffisant. Le Secrétariat d'État aux questions financières internationales (SFI) vérifie ces exigences et a sollicité à plusieurs reprises notre avis sur les questions relatives à la protection des données.

Nous l'avons rendu attentif au fait qu'aucune garantie supplémentaire n'est nécessaire dans le cadre de l'activation bilatérale d'un EAR avec une juridiction étrangère bénéficiant d'un niveau de protection adéquat conformément à la liste des États publiée sur notre site Internet. Toutefois, en ce qui concerne les pays ne disposant pas de ce statut, des garanties supplémentaires doivent être prévues.

Un panel constitué de douze experts, principalement informaticiens, a été mandaté par l'OCDE pour évaluer la confidentialité et le respect du principe de spécialité de diverses juridictions étrangères notamment sur la base de questionnaires-types figurant à l'annexe 4 du CRS. Ceux-ci thématisent essentiellement des aspects techniques et de sécurité de l'information. Des visites locales dans ce contexte ne sont en règle générale pas à l'ordre du jour. En outre, les droits découlant du respect du droit fondamental à la sphère privée tels que le droit à la rectification, le droit d'accès et le droit à l'effacement des données n'y sont pas examinés. Par conséquent, le questionnaire est un outil incomplet qui ne permet pas d'évaluer dans son ensemble le niveau de protection des données personnelles d'une juridiction étrangère. Nous avons indiqué au SFI que l'activation d'un EAR avec un État

tiers sans prévoir de garanties supplémentaires comporte des risques, malgré une bonne notation du panel d'expert.

d. Arrêté fédéral concernant l'introduction de l'EAR avec l'Australie

Comme indiqué ci-dessus le MCAA et le projet de LEAR déterminent les fondements juridiques de l'EAR, sans définir les États avec lesquels il sera introduit. L'Australie est un des partenaires avec lesquels la Suisse a souhaité introduire l'EAR avec un premier échange prévu en 2018. Le projet est passé en consultation dans le courant 2015 et nous avons eu l'occasion d'émettre quelques remarques à ce sujet. Nous avons en particulier relevé qu'il convenait de vérifier si le secteur fiscal est couvert par la législation australienne régissant le droit à la vie privée et, le cas échéant, si elle couvre les données des étrangers et des personnes morales.

D'après l'analyse du DFF dans sa proposition au Conseil fédéral, la législation australienne offre des garanties appropriées en matière de protection des données dans le cadre de l'introduction de l'EAR avec l'Australie.

e. Arrêté fédéral sur l'approbation d'un protocole d'amendement de l'accord sur la fiscalité de l'épargne entre la Suisse et l'UE

L'activation bilatérale de l'EAR avec l'UE a été signée le 27 mai 2015. En l'espèce, le procédé est différent de celui comprenant une activation par le biais du MCAA comme pour l'Australie. En l'occurrence, l'accord préexistant sur la fiscalité de l'épargne entre la Suisse et l'UE a pu être utilisé pour mettre en œuvre l'EAR. Pour ce faire, un protocole d'amendement a été prévu. Ce dernier transforme, sur le plan matériel, presque intégralement l'accord sur la fiscalité de l'épargne en un accord sur l'EAR.

Lors de la consultation, nos remarques ont particulièrement porté sur la garantie du respect de la finalité des traitements uniquement à des fins fiscales. Le DFF en a partiellement tenu compte.

1.9.3 Assouplissement de l'assistance administrative pour les données volées

Nous estimons que le traitement des demandes d'assistance administrative reposant sur des données volées enfreint le principe de licéité. Nous nous sommes donc exprimés de manière critique dans la procédure de consultation concernant une nouvelle modification de la loi sur l'assistance administrative en matière fiscale.

Outre la modification de la loi sur l'assistance administrative en matière fiscale qui est discutée au chiffre 1.9.2 du présent rapport d'activités, un autre amendement du texte est encore prévu. N'ayant pas été sollicité dans le cadre de la consultation interne des offices, nous nous sommes exprimés lors de la procédure de consultation externe. Nous estimons que la modification prévue est extrêmement problématique du point de vue du droit de la protection des données. Si des données sont acquises de manière illicite puis transmises, le destinataire des informations personnelles qui en réalise également le traitement enfreint le principe de légalité et porte atteinte à la personnalité de la personne concernée. Selon nous, ce caractère illicite ne peut être justifié par une distinction entre agissements actifs et passifs de l'État du destinataire. Si un État accepte les données volées qui lui sont proposées, il accepte ainsi leur passé délictuel. S'il les traite et les transfère, il agit là aussi de manière illégale et participe aux atteintes à la personnalité. Par conséquent, nous avons prié le SFI de supprimer ou de modifier le projet de loi, ce qui n'a pas été considéré.

1.9.4 Banques et droit d'accès

Nous recevons de plus en plus de requêtes concernant le droit d'accès octroyé par les banques. Certains établissements exigent pour cela une participation aux frais qui dépasse largement le montant de 300 francs autorisé par le droit de la protection des données.

Nous recevons de plus en plus de demandes concernant le droit d'accès au sens de l'article 8 de la loi sur la protection des données (LPD) auprès des banques. Certains établissements financiers, en particulier, semblent ne pas vouloir répondre à de telles requêtes, ou sous condition du paiement de participations aux frais élevées.

Le droit d'accès est le point de départ de l'application d'autres droits relatifs à la protection des données, tels que les droits de rectification, de blocage ou de suppression des données personnelles. Il ne peut être restreint que dans des conditions très précises. Si une banque limite l'accès, elle doit en communiquer le motif. Par ailleurs, elle se rend coupable si elle fournit de manière intentionnelle des

renseignements inexacts ou incomplets. L'accès peut par exemple être restreint si la personne concernée agit de manière abusive. Le Tribunal fédéral a placé à un niveau élevé, dans l'ATF **138** III 425, les exigences visant à éviter les abus relatifs au droit d'accès. Par cet arrêt, une banque est tenue de fournir des renseignements même si les informations en question sont demandées non seulement pour des raisons liées au droit de la personnalité, mais aussi pour les faire éventuellement valoir dans une procédure consécutive relevant du droit de la responsabilité civile. Il semble que pour certains établissements financiers, la solution trouvée face à ce dilemme réside à présent dans un octroi de renseignements à un prix exorbitant. Le montant des participations aux frais que la LPD autorise repose sur une base légale claire: le détenteur des données, c'est-à-dire la banque, peut exiger au maximum 300 francs. Nous conseillons donc en ce sens les personnes concernées. Elles peuvent en outre faire valoir leur droit d'accès devant le juge civil.

1.10 International

1.10.1 Coopération internationale

La coopération internationale entre autorités de protection des données demeure une activité essentielle pour assurer une assise la plus large possible du droit à la protection des données. Le PFPDT s'implique activement dans les travaux du Conseil de l'Europe, de l'Organisation de coopération et de développement économique (OCDE), de la conférence européenne et de la conférence internationale des commissaires à la protection des données, ainsi qu'au sein de l'Association francophone des autorités de protection des données (AFAPDP). Dans le cadre des accords d'association Schengen-Dublin, il participe aux travaux de différents groupes de coordination au sein de l'Union européenne.

Conseil de l'Europe

Les travaux de modernisation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) qui doit déboucher sur l'adoption d'un protocole d'amendements font partie des objectifs prioritaires de l'organisation dans le domaine de la protection des données. Ces travaux sont néanmoins gelés depuis fin 2014 dans l'attente de la finalisation du nouveau cadre juridique de l'Union européenne. L'adoption au début 2016 du projet de règlement européen de protection des données et de la directive sur les transferts de données à des fins policières et judiciaires devrait permettre de terminer la révision. Parallèlement, le Conseil de l'Europe poursuit sa politique de promotion de la Convention 108 auprès des États tiers. Outre l'Uruguay qui a adhéré en 2013, le Maroc, l'île Maurice, le Sénégal, la Tunisie, suite à un avis positif du comité consultatif (T-PD), ont été invités par le comité des Ministres à adhérer. Avec l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 invalidant la décision 200/520 de la Commission européenne relative à la sphère de sécurité (l'accord Safe Harbor) avec les États-Unis, il apparaît plus que jamais nécessaire que chaque État mette en place un système de protection effectif basé sur des principes communs et universellement reconnus. La Convention 108 de par sa vocation universelle offre ainsi une opportunité au Conseil de l'Europe de renforcer son rôle pionnier dans la communauté internationale de la protection des données.

Le T-PD a tenu sa 32^{ème} réunion plénière à Strasbourg du 1^{er} au 3 juillet 2015. Il a en particulier examiné la Recommandation 2067 (2015) de l'Assemblée parlementaire sur les opérations de surveillance massive et adopté un avis. Dans cet avis, il invite le Conseil de l'Europe à redoubler d'efforts pour promouvoir la Convention 108,

en vue de l'adhésion d'États tiers, notamment de ceux qui sont déjà Parties à la Convention sur la cybercriminalité. Il rappelle que le droit fondamental au respect de la vie privée est protégé par la Convention 108 et son protocole additionnel. Le travail de modernisation devrait renforcer l'efficacité de cet outil au niveau mondial. Il soutient l'appel à adresser une recommandation aux États membres en vue de garantir la protection de la vie privée à l'ère du numérique et la sécurité d'internet à la lumière des menaces que représentent les techniques de surveillance massive. Il se réjouit également de l'appel à étudier les problèmes de sécurité sur internet que posent les pratiques de surveillance massive, ainsi que l'appel à étudier les menaces découlant de ces pratiques. Il rappelle à cet égard que, en l'absence de tout mécanisme de contrôle, le traitement de données à caractère personnel risque de compromettre la jouissance d'autres droits fondamentaux, ainsi que d'autres intérêts légitimes. Enfin, le comité soutient la proposition de créer un code destiné aux services de renseignement et contribuera le cas échéant à tous travaux futurs.

Le T-PD a en outre entamé des travaux en vue de l'élaboration d'un guide pratique concernant la protection des données dans le secteur de la police. Il s'est engagé dans la révision de la recommandation R (97) 5 relative à la protection des données médicales. Il s'agit en particulier de tenir compte des évolutions technologiques, notamment le développement des dossiers électroniques du patient, les consultations à distance, l'arrivée de l'internet des objets (par exemple «le soi quantifié»), avec des acteurs qui n'appartiennent pas au monde traditionnel de la santé et du domaine médical. Le comité a débattu des enjeux des mégadonnées pour la protection des données et décider d'élaborer des lignes directrices. Il a examiné un rapport sur les données des passagers (PNR) et chargé son bureau d'élaborer un avis. Enfin, il a estimé nécessaire de poursuivre l'examen des questions de protection des données liées à l'échange automatique de données à des fins administrative et fiscale.

Conférence européenne des commissaires à la protection des données

La conférence européenne des commissaires à la protection des données s'est déroulée du 18 au 20 mai 2015 à Manchester à l'invitation de l'Office du commissaire à l'Information du Royaume-Uni. La Conférence a permis aux participants d'échanger sur les pratiques en matière de protection des données dans le monde numérique (notamment en matière de sensibilisation, de traitement des plaintes et de coopération). La conférence a ainsi pris connaissance d'une [étude relative aux droits des personnes concernées et aux attentes du public envers les autorités de protection des données](#). L'étude souligne qu'il est important que les autorités, pour être effectives, aient connaissance des attentes du public en matière de protection

des données et sachent comment les personnes comprennent leurs droits et souhaitent les exercer. Celles-ci aspirent notamment à avoir le contrôle sur les données qui les concernent, attendent une plus grande transparence sur les traitements, et voudraient mieux comprendre les finalités poursuivies et les bénéfiques de l'échange de données. Le public en général attend des autorités de protection des données en particulier qu'elles agissent en toute indépendance, assurent leur visibilité et fassent usage de leurs pouvoirs pour faire respecter les règles de protection des données, y compris en rendant public leurs rapports d'investigation. Les autorités devraient plus anticiper l'arrivée de nouvelles technologies. Plusieurs autorités ont mis le doigt sur l'insuffisance des ressources et l'impossibilité de donner suite à toutes les demandes et plaintes qui leur sont adressées.

Conférence internationale des commissaires à la protection des données

La 37^e Conférence internationale des commissaires à la protection des données s'est tenue à Amsterdam, du 26 au 29 octobre 2015, à l'invitation de l'autorité néerlandaise de protection des données. Placée sous le thème des ponts à construire, la conférence ouverte, qui a rassemblé quelques 700 participants issus des autorités de protection des données et de représentants de l'économie, des administrations publiques, des organisations internationales, de la société civile et du monde académique, a examiné un rapport préparé par des experts américains et européens. Ce rapport propose dix pistes pour améliorer la protection des données dans les relations transatlantiques. Le rapport a reçu un accueil peu enthousiaste de la part de plusieurs participants regrettant notamment son orientation trop atlantiste et l'absence de propositions de changements législatifs. Pour leurs auteurs cependant, ces propositions sont applicables dans le respect du cadre actuel de protection des données et peuvent être transposées dans d'autres régions du monde. Ces différentes propositions seront approfondies et pourraient déboucher sur des projets concrets à l'avenir.

Dans la partie de la conférence réservée aux autorités de protection des données, celles-ci ont débattu de la manière de répondre aux changements intervenant dans le monde en particulier marqué par un environnement sécuritaire. Il s'agit en particulier d'assurer la confiance du public, notamment en exigeant la transparence sur les activités de renseignements. Les agences de renseignements et de sécurité doivent agir dans le respect des lois et notamment limiter l'utilisation de leurs pouvoirs intrusifs au strict nécessaire. Les autorités de protection des données ont également abordé la question du traitement des données génétiques. Bien qu'il existe de nombreux avantages du partage d'informations génétiques, l'utilisation

de ces données comportent de nombreux risques qui dépendent, dans une large mesure, du contexte dans lequel ces données sont traitées et des garanties offertes lors de leur traitement.

Il apparaît ainsi crucial que les personnes concernées puissent garder le contrôle de leurs données, qu'elles reçoivent des informations appropriées et que leur choix soient respectés. Cela peut être effectué grâce à divers moyens permettant d'assurer une gestion dynamique du consentement tout au long du cycle de vie des données, et complété par des garanties supplémentaires. Il convient aussi de prendre en considération que les données génétiques révèlent des informations sur autrui, contribuant à leur identification et leur caractérisation. Si l'innovation ne doit pas être freinée par la protection des données, elle doit néanmoins se faire dans un cadre garantissant les droits et les libertés fondamentales des personnes concernées.

Les autorités de protection des données ont adopté [quatre résolutions](#) relatives à l'orientation stratégique de la conférence, à la coopération avec le rapporteur spécial de l'ONU sur le droit à la vie privée, sur la transparence et l'action humanitaire internationale. Par cette dernière résolution, les autorités de protection des données s'engagent à analyser les exigences en la matière dans le contexte de l'action humanitaire et à répondre à la demande de coopération des acteurs humanitaires pour développer des lignes directrices prenant en considération les spécificités de l'action humanitaire internationale. Un groupe de travail ad hoc a été créé pour mener ces activités. Ce groupe est coordonné conjointement par l'autorité espagnole de protection des données et le PFPDT. Il rendra compte de ses travaux à l'occasion de la prochaine conférence internationale des commissaires à la protection des données et à la vie privée qui se tiendra à Marrakech au Maroc en 2016.

En outre, [l'entente sur la coopération entre autorités de protection des données](#) adoptée lors de la 36^e conférence est entrée en vigueur le 27 octobre 2015. Le PFPDT n'a pas encore été en mesure de s'associer à cette déclaration d'intention non contraignante du fait d'un préavis négatif de l'Office fédéral de la justice, qui estime que nous n'avons pas la compétence pour signer un tel engagement.

À l'issue de la conférence, une [déclaration finale](#) a été publiée.

Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP) s'est réunie en conférence les 25 et 26 juin 2015 à Bruxelles. À cette occasion, les participants ont débattu de la surveillance et des droits numériques. Concernant la surveillance, les autorités ont rappelé qu'un équilibre des intérêts entre protection

des données et sécurité doit absolument être maintenu. Cet équilibre passe par l'adoption d'un cadre commun et un contrôle indépendant des activités de surveillance. Concernant les droits des individus dans l'univers numérique, nous avons eu l'occasion de présenter la réglementation du droit à l'oubli en droit européen et notamment [l'arrêt de la Cour de justice de l'Union européenne du 13 mai 2014](#). À l'issu des discussions, il est apparu nécessaire d'offrir aux personnes une réelle maîtrise sur leurs données sans pour autant évoluer vers une patrimonialisation des données personnelles. Il s'agit aussi d'encourager une prise de conscience collective et individuelle de l'importance de protéger ses données personnelles. Les participants ont également assisté à plusieurs ateliers consacrés notamment au contrôle de la conformité des traitements, à l'amélioration du traitement des plaintes et à la coopération.

Les membres de l'AFAPDP ont adopté deux résolutions qui portent sur [la surveillance de masse](#) et sur [la prise en compte de l'éthique dans le traitement des données de santé et les données génétiques](#).

Les groupes de coordination des contrôles SIS II, VIS et Eurodac, et l'évaluation Schengen de l'Autriche et du Liechtenstein

En 2015, les groupes de coordination des contrôles du système d'information Schengen de deuxième génération (SIS II), du système d'information sur les visas (VIS) et de la banque de données européenne des empreintes digitales (Eurodac) se sont réunis à deux reprises. Par ailleurs, nous avons participé aux évaluations Schengen de l'Autriche et du Liechtenstein en tant qu'experts.

Les groupes de coordination du contrôle relatif au SIS II, au VIS et à l'Eurodac se sont réunis les 25 et 26 mars 2015 et les 7 et 8 octobre 2015 à Bruxelles.

Au cours de la rencontre de mars, le Royaume-Uni (GB) a été admis au sein du groupe de coordination du contrôle du SIS II comme membre à part entière. En effet, il participe depuis peu à une partie de Schengen (participation au système d'information SIS II). De plus, le groupe de coordination du contrôle du SIS II a adapté le guide concernant l'exercice du droit d'accès. Le groupe de coordination de contrôle du VIS a établi son rapport d'activités 2012-2014. Pour sa part, le groupe de coordination du contrôle de l'Eurodac a entre autres abordé la question de l'entrée en matière de la nouvelle ordonnance européenne Eurodac, sur laquelle est basé l'accès des autorités de poursuite pénale à Eurodac. En septembre 2015, un sous-groupe des groupes de coordination de contrôle a visité les systèmes d'information SIS II, VIS et Eurodac à Strasbourg; ils se sont surtout penchés sur les aspects touchant à la sécurité des données.

En 2015, nous avons également participé à titre d'experts aux évaluations Schengen dans le domaine de la protection des données: en mars à l'évaluation de l'Autriche et en novembre à celle de la Principauté du Liechtenstein. L'Autriche était le premier pays à être évalué depuis la mise en place du nouveau mécanisme qui contient quelques modifications. Désormais, il y a deux experts principaux, l'un représentant la Commission européenne, l'autre les États membres. Le rapport d'évaluation des experts peut, sur les différents points, aboutir aux résultats suivants: conforme, non conforme et conforme mais nécessitant des améliorations. De plus, les recommandations ne figureront plus désormais dans le rapport annuel, mais dans un document séparé.

Groupe de travail «Border, Travel & Law Enforcement»

Le «Border, Travel & Law Enforcement subgroup» (BTLE) est un sous-groupe créé par le Groupe de travail «article 29» sur la protection des données. Le sous-groupe a pour mission de suivre les développements législatifs touchant aux secteurs de la police, des frontières et de la justice pénale, notamment ceux relevant de l'acquis Schengen. Dans ce contexte, il prépare des avis et des positions qui sont ensuite adoptés par le groupe de travail «article 29». Nous avons participé aux différentes réunions au cours de l'année sous revue.

Suite à l'arrêt du 6 octobre 2015 de la Cour de justice de l'Union européenne dans l'affaire n° C-362/14, Schrems c. Data Protection Commissioner, le sous-groupe de travail a reçu le mandat d'analyser la législation américaine et d'identifier les exigences minimales à respecter en cas d'atteinte à la vie privée dans le cadre des activités des services de renseignements.

Le sous-groupe de travail a par ailleurs poursuivi l'examen de l'arrêt de justice de l'Union européenne concernant la conservation des données personnelles aux fins de lutte contre le crime organisé et le terrorisme. Dans ce contexte, il a élaboré un questionnaire afin de recenser les pratiques dans les différents États membres.

Le sous-groupe suit avec une attention particulière l'avancée du projet de «frontières intelligentes» suite à l'adoption par la Commission européenne d'une proposition de règlement portant sur la création d'un système pour l'enregistrement des entrées et sorties des ressortissants d'États tiers franchissant les frontières extérieures des États membres de l'Union européenne et d'un règlement portant sur la création d'un programme d'enregistrement des voyageurs.

Enfin, le sous-groupe de travail accompagne la création d'un cadre européen pour la communication des données PNR aux États tiers et pour l'utilisation de ces

données à des fins répressives. Il observe également attentivement l'évolution de la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

Groupe de coordination des autorités suisses de protection des données dans le cadre de Schengen

Par le biais du «groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en œuvre de l'accord d'association à Schengen», nous coordonnons avec les autorités cantonales de protection des données nos activités de surveillance des traitements de données effectués en Suisse en matière de migration, police et justice, en application de la coopération Schengen.

Le groupe de coordination des autorités suisses de protection des données s'est réuni deux fois en 2015.

La première réunion a eu lieu sous forme d'une visite à des fins de formation que nous avons organisée auprès du bureau SIRENE (interlocuteur national chargé de l'échange des informations supplémentaires). Les participants ont pu à cette occasion poser leurs questions à la conseillère à la protection des données et au chef du bureau SIRENE.

Lors de la deuxième réunion, nous avons informé les autorités cantonales de protection des données des principaux points abordés par le groupe de coordination de contrôle du SIS II ainsi que des différents contrôles que nous allons mener. Les cantons ont pour leur part présenté les résultats de leurs activités de contrôle. Afin de simplifier l'analyse des logfiles du SIS, nous avons mis à disposition des autorités cantonales un outil informatique que nous avons créé.

Groupe de travail international sur la protection des données dans les télécommunications

Le PFPDT a participé les 13 et 14 octobre 2015 à la 58^e séance du groupe de travail international pour la protection des données dans les télécommunications (International Working Group on Data Protection in Telecommunications, IWGDPT). Les thèmes suivants ont notamment été abordés, sous la présidence du chargé de la protection des données et de la liberté de l'information berlinois: systèmes

d'authentification biométriques, protection des données sur les plates-formes d'e-learning, suivi sur le web (problématique «do-not-track»), protection des données sur les réseaux sociaux, et téléviseurs «intelligents». Les documents de travail et positions communes du groupe peuvent être consultés (en anglais) sur le site Internet suivant: www.datenschutz-berlin.de

En outre, nous nous sommes également informés sur les évolutions et les débats autour de la conservation des données, notamment aux États-Unis, au Canada, en Grande-Bretagne et en Allemagne, à l'occasion d'un séminaire de l'Académie européenne pour la liberté d'information et la protection des données (EAID), également organisé à Berlin, le 14 octobre 2015.

2. Principe de la transparence

2.1 Demande d'accès

Selon les chiffres qui nous ont été communiqués, 597 demandes d'accès ont été soumises aux autorités fédérales en 2015 (avec le Ministère public de la Confédération et les Services parlementaires, les demandes d'accès s'élèvent à 600, cf. chiffre 2.1.2 s.). Cela correspond à une nouvelle valeur record depuis l'entrée en vigueur de la loi sur la transparence en 2006. Les autorités ont accordé dans 319 cas (54 %) un accès complet et dans 127 autres cas (21 %) un accès partiel aux demandeurs. En revanche, la demande de consultation a été entièrement rejetée pour 98 demandes (16 %). Par ailleurs, 31 demandes d'accès ont été retirées et 22 cas étaient encore en suspens à la fin de l'année 2015. Etant donné l'augmentation continue du nombre des demandes d'accès, il faut s'attendre à ce qu'à l'avenir la loi sur la transparence continue à être mieux connue et davantage utilisée.

En ce qui concerne le nombre total de demandes d'accès et la pratique des autorités à cet égard, les chiffres sont globalement stables par rapport aux années précédentes. L'accès a été accordé dans presque la moitié des cas, dans un quart il a été partiellement refusé et entièrement refusé pour le reste.

2.1.1 Départements et offices fédéraux

Au niveau des offices, c'est le CDF qui a reçu le plus de demandes d'accès en 2015 (43), suivi de l'OFEV (31), de l'OFAG et de la COMCO (23 chacun), ainsi que de l'OFSP et du SG-DDPS (22 chacun). Dans le peloton de tête des départements figurent le DFAE (134 demandes), le DETEC (101) et le DFF (84). Les chiffres du DFAE témoignent d'une grande ouverture à la transparence avec 110 réponses entièrement positives sur 134 demandes; dans 17 cas, l'accès a été partiellement accordé ou repoussé et dans 7 cas seulement entièrement refusé. Sur 71 autorités, 17 nous ont annoncé qu'aucune demande ne leur avait été soumise pendant l'année 2015. Le Préposé lui-même a reçu 7 demandes en 2015 auxquelles il a accordé un accès complet.

Le montant total des émoluments liés à l'accès à des documents officiels et prélevés au cours de l'année sous revue s'élève à 13 663 francs. Il s'agit donc d'un montant considérablement plus élevé par rapport aux autres années (2012: 6 322 fr.; 2013: 6 502 fr.; 2014: 2 600 fr.). Ce montant ne correspond qu'à 17 seulement des 597 demandes d'accès déposées au total. Comme au cours des années précédentes, aucun émoulement n'est requis dans la plupart des cas (en moyenne dans 97 %). Il convient de noter tout particulièrement la permanence des différences

dans la pratique en matière d'émoluments entre les différentes autorités. Alors que la Chancellerie fédérale et trois départements n'ont prélevé aucun émolument, quatre autres ont partiellement facturé leur temps de travail aux demandeurs. La majeure partie des montants facturés l'ont été par le DDPS (5 663 fr. pour 5 demandes), le DETEC (4 150 fr. pour 3 demandes) et le DEFRR (3 650 fr. pour 8 demandes). Ne sont pas compris dans le total mentionné plus haut les cas dans lesquels les éventuels émoluments n'ont pas encore été fixés de manière définitive au cours de l'année écoulée. Cela concerne par exemple un cas examiné par le Tribunal administratif fédéral dans lequel le tribunal a réduit le montant des émoluments demandés de 16 500 francs (coût total estimé par les autorités pour le traitement de la demande d'accès) à un maximum de 8 500 francs (jugement A-2589/2015 du 4 novembre 2015).

En ce qui concerne les heures de travail que représente le traitement des demandes, le Préposé souligne à nouveau que les autorités ne sont pas tenues de les enregistrer et qu'il n'existe aucune directive de saisie uniforme pour l'ensemble de l'Administration fédérale. Les indications qui lui sont transmises sur une base volontaire ne sont donc que partiellement pertinentes. Selon ces données, le temps de travail annoncé a considérablement augmenté par rapport aux années précédentes (2012: 2155 heures; 2013: 1707 heures; 2014: 1642 heures; 2015: 2912 heures). En revanche, le temps de travail investi dans la participation à des procédures de médiation est en diminution: il est passé de 1436 heures en 2014 à 1148 heures en 2015. Par contre, le temps de travail consacré à l'établissement d'une décision ou à une éventuelle procédure de recours n'a pas été comptabilisé ou n'a pas été comptabilisé séparément.

2.1.2 Services parlementaires

Les services parlementaires nous ont annoncé deux demandes d'accès en 2015. Dans un cas, l'accès aux documents a été entièrement accordé et dans l'autre cas entièrement refusé.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a annoncé une seule demande d'accès pour 2015 pour laquelle l'accès a été partiellement accordé.

2.2 Demandes en médiation

En 2015, 98 demandes en médiation ont été soumises, ce qui constitue une augmentation de quelque 9 % (90 demandes en 2014). De même que l'année précédente, la plupart des demandes déposées en 2014 provenaient de professionnels des médias (26), suivis par les particuliers (23).

Ces chiffres permettent d'émettre les conclusions et les remarques suivantes: dans 225 cas, l'Administration fédérale a refusé l'accès de manière totale (98) ou partielle (127). Ces données sont à mettre en perspective avec les 98 demandes en médiation qui nous sont parvenues. Pendant l'année sous revue, une demande en médiation a donc été soumise dans plus de 43 % des cas de demandes d'accès totalement ou partiellement rejetées (2014: 36 %).

Au total, 134 demandes en médiation ont été réglées en 2014, dont 59 avaient été soumises pendant cette même année, 52 en 2014, 21 en 2013 et 2 en 2012. Dans 35 cas, une solution consensuelle a été trouvée entre les parties, 19 ayant permis de parvenir à une médiation au sens propre et les 16 procédures restantes ayant été résolues à l'amiable grâce à l'intervention du Préposé. Dans 4 cas, l'accès a été autorisé après ouverture de la procédure de médiation sans intervention du Préposé. Le Préposé a émis en tout 58 recommandations lorsqu'aucune solution amiable n'était envisageable de prime abord. Ces 58 recommandations ont permis de liquider 83 demandes en médiation. Par ailleurs, 4 demandes en médiation ont été retirées. Dans 2 cas, les conditions d'application de la LTrans n'étaient pas remplies. Dans 5 autres, la demande en médiation n'avait pas été soumise dans les délais. Enfin, une procédure de médiation a été suspendue.

Pendant l'année sous revue, le nombre de procédures de médiation menées à terme a considérablement augmenté, ce qui s'explique en premier lieu par la présence de deux collaborateurs supplémentaires dont le poste était limité à fin 2015. Toutefois, les retards importants accumulés dans le traitement des procédures de médiation en suspens n'ont pas pu être entièrement résorbés.

Toutes les recommandations émises pendant l'année sous revue sont disponibles [sur le site Internet du Préposé](#).

2.3 Consultations des offices et autres prises de position

2.3.1 Coopération au sein du groupe de travail Transparence et révision partielle de la loi sur la transparence

Le Conseil fédéral entend améliorer la mise en œuvre de la loi sur la transparence. À la suite de l'évaluation, il a d'une part décidé que la loi sur la transparence sera partiellement révisée et a d'autre part constitué un groupe de travail interdépartemental. Ce groupe de travail a pour tâche d'améliorer les échanges au sein de l'administration fédérale; il doit également être intégré à l'élaboration de l'avant-projet.

Dans son dernier rapport d'activités ([22^e Rapport d'activités](#) 2014/2015, p. 88 ss), le Préposé a fait état de l'évaluation menée par l'Office fédéral de la justice (OFJ); le Conseil fédéral a pris connaissance des résultats de cette évaluation au cours de l'année écoulée. Il veut améliorer la mise en œuvre du principe de la transparence dans l'administration fédérale et, à cet effet, a chargé le Département fédéral de justice et police (DFJP) de préparer un avant-projet de révision partielle de la loi sur la transparence (LTrans). Ainsi, les entreprises dont les secrets d'affaires et de fabrication sont ou pourraient être concernés par des demandes d'accès doivent être mieux impliquées dans la procédure de demande d'accès. Il conviendrait en outre de réfléchir à la manière de clarifier les rapports entre la loi sur la protection des données (LPD) et la LTrans. Enfin, le DFJP doit examiner des solutions permettant de raccourcir la procédure de médiation.

Par ailleurs, le Conseil fédéral a décidé de créer un groupe de travail interdépartemental placé sous l'égide de l'OFJ. Ce groupe de travail, intitulé «Transparence», doit assurer les échanges entre les conseillers à la transparence de l'administration fédérale et contribuer à améliorer la mise en œuvre de la LTrans. Le Préposé est représenté dans ce groupe de travail, aux côtés des conseillers à la transparence des départements, de la Chancellerie fédérale, des Services du Parlement, des Archives fédérales ainsi que d'un représentant de la Conférence des Services d'information de la Confédération (CSIC).

En 2015, ce groupe de travail s'est réuni à deux reprises pour discuter des solutions proposées par l'OFJ sur les différents points de la révision. Le Préposé s'est également exprimé dans ce groupe contre les limitations au principe de la transparence. Ainsi, il s'oppose à l'exemption du champ d'application de la LTrans pour les rapports

de surveillance, d'inspection, d'audit ou de contrôle des autorités fédérales concernées. En outre, le Préposé estime que la coordination entre la LTrans et la LPD est d'ores et déjà assez clairement définie. La pratique en matière de recommandation du Préposé et le nombre croissant des arrêts des tribunaux fédéraux contribuent aussi à clarifier la question de l'accès aux documents officiels comportant des données personnelles, car il en résulte une meilleure sécurité juridique.

Depuis l'entrée en vigueur de la LTrans, le délai de 30 jours pour l'accomplissement de la procédure de médiation donne lieu à discussion. Dans la majorité des cas, le Préposé ne peut pas respecter ce délai et a déjà été rappelé à l'ordre à ce propos par le Tribunal administratif fédéral pour retard injustifié. L'expérience montre que le délai de 30 jours n'est pas réaliste en pratique. De l'avis du Préposé, la fixation d'un délai contredit fondamentalement la nature de la procédure de médiation. Le Préposé a une position claire quant au mandat donné par le Conseil fédéral d'examiner les solutions permettant de raccourcir la durée des procédures de médiation: la seule manière de réduire véritablement cette durée est d'octroyer des ressources suffisantes (cf. chiffre 2.1 du présent rapport d'activité). Toute autre nouvelle réglementation légale visant à raccourcir les procédures de médiation risquent de nuire au principe de la transparence au détriment du requérant.

2.3.2 Organisation de l'infrastructure ferroviaire

Nous nous sommes prononcés, dans le cadre de la consultation des offices, sur le projet «Organisation de l'infrastructure ferroviaire» de l'Office fédéral des transports (OFT). Ce projet prévoyait une large réduction de la transparence dans le domaine de la surveillance légale de l'OFT. Nous avons pris position sur les dispositions législatives prévues dans quatre textes de loi.

L'OFT avait prévu quatre dispositions spéciales identiques dans la loi fédérale sur les chemins de fer (LCdF), la loi fédérale sur les installations à câbles transportant des personnes (LICa), la loi fédérale sur le transport des voyageurs (LTV) et la loi fédérale sur la navigation intérieure (LNI). Conformément à ces dispositions, la loi sur la transparence (LTrans) ne s'appliquera plus aux rapports concernant les audits, les contrôles d'exploitation et les inspections de l'OFT, ainsi qu'à tous les autres documents concernant la sécurité technique ou la sécurité de l'exploitation s'ils contiennent des données personnelles.

Nous avons rejeté ces projets de dispositions car la LTrans ne définit pas de catégories de documents officiels qui, d'emblée, ne seraient pas accessibles (par ex. les rapports d'audit ou d'inspection). En outre, la LTrans contient suffisamment de

dispositions dérogatoires qui sont autant de possibilités de tenir compte du besoin de protection accru de certains documents officiels. Par ailleurs, nous avons rappelé les devoirs de participation des entreprises placées sous la surveillance légale de l'OFT, devoirs qui ne sont pas remis en question par la LTrans. Ainsi, le législateur a délibérément établi que la confidentialité entre les autorités de surveillance et les entreprises surveillées n'est pas une clause d'exception prévue par la LTrans.

Enfin, nous avons aussi rejeté les dispositions concernées en raison du fait que l'OFT, outre les rapports proprement dits d'audit, de contrôle et d'inspection, entendait également excepter du droit à l'accès tous les autres documents officiels dans la mesure où ils contiennent des données personnelles portant sur la sécurité technique ou la sécurité de l'exploitation. L'ensemble de l'activité de surveillance de l'OFT se soustrairait ainsi intégralement à la LTrans contrairement à la volonté du législateur.

Nous constatons avec préoccupation que d'autres unités administratives (notamment des autorités de surveillance) tentent de profiter de révisions de loi pour soustraire des pans de leur activité ou certaines catégories de documents du champ d'application de la LTrans.

2.3.3 Libre accès aux données publiques / Open Government Data (OGD)

Le 16 avril 2014, le Conseil fédéral a adopté la stratégie de libre accès aux données publiques en Suisse pour la période 2014-2018, avec laquelle il entend développer le libre accès aux données des autorités. La stratégie a été élaborée sous la direction de l'Unité de pilotage informatique de la Confédération (UPIC). Depuis début 2015, les Archives fédérales sont chargées de la mise en œuvre de cette stratégie et élaborent les bases conceptuelles nécessaires. Dans ce contexte, nous avons été priés de nous prononcer sur le cadre réglementaire des données publiques en libre accès du point de vue du principe de la transparence.

Nous approuvons tous les efforts politiques déployés en faveur d'un accès libre et simple aux données publiques. Nous estimons en particulier que la mise en place à l'échelle nationale d'une plateforme pour les données publiques en libre accès constitue un élargissement utile et nécessaire des droits de la population à l'information. Un accès plus large aux informations des autorités administratives renforce la confiance dans les institutions étatiques et permet une participation judicieuse au processus politique de décision.

Sous l'angle du principe de transparence, nous avons souligné que le libre accès aux données publiques en tant que pratique d'information active (information volontaire ou prévue par la loi) doit être strictement séparé de la loi sur la transparence (LTrans) qui régit uniquement l'activité passive d'information des autorités (information sur demande). Il ressort également de cette séparation nette entre les deux modes d'information des autorités qu'il est impossible de fonder juridiquement le libre accès aux données publiques sur la LTrans. - Nos remarques en matière de protection des données sur le libre accès aux données publiques se trouvent au chiffre 1.1.2 du présent rapport d'activités.

2.3.4 Révision de l'ordonnance sur l'énergie et de l'ordonnance sur l'approvisionnement en électricité

L'Office fédéral de l'énergie a clarifié sa pratique concernant la publication de certaines données sur les installations recevant une rétribution.

Dans le cadre de la procédure de consultation, le Préposé a pris position sur le projet de révision de l'ordonnance sur l'énergie (OEne) et de l'ordonnance sur l'approvisionnement en électricité (OApE).

Le projet de révision prévoyait de clarifier la situation, en réglant de manière explicite la pratique existante de publier un certain nombre de données concernant les installations qui sont en droit de recevoir une rétribution, telles que le nom des producteurs, l'emplacement de l'installation, la source d'énergie, la puissance, la production, le montant de la rétribution, etc. Pour les installations possédant une puissance inférieure à 30 kW, la publication reste anonyme.

Le Préposé a salué la volonté de l'Office fédéral de l'énergie de prévoir la publication active de certaines données concernant les installations qui reçoivent une rétribution dans l'ordonnance. Toutefois il a considéré que dans l'intérêt de la transparence, cette publication devait revêtir un caractère obligatoire. Ensuite, en lien avec la publication anonymisée des données pour les installations d'une puissance inférieure à 30 kW, il a rappelé qu'une demande d'accès à ces informations basée sur la loi sur la transparence reste possible et qu'il conviendrait de le préciser dans la note explicative.

Par la suite, l'Office fédéral de l'énergie a informé le Préposé qu'il était d'accord avec l'ensemble des remarques et qu'il modifierait dans ce sens le projet de révision ainsi que la note explicative. La révision est entrée en vigueur le 1^{er} janvier 2016.

2.3.5 Loi sur l'information et l'accès aux documents du canton de Fribourg

Le Préposé a été appelé à se prononcer sur l'avant-projet de loi sur l'information et l'accès aux documents (LInf) dans le cadre de la procédure de consultation. Il approuve chaque pas fait en direction d'une plus grande transparence et se prononce en faveur de la proposition principale.

Par cette modification, le canton de Fribourg entend adapter sa loi sur l'information à la Convention d'Aarhus. Cette convention, en vigueur en Suisse depuis le 1^{er} juin 2014, se compose de trois éléments majeurs. En premier lieu, elle donne à tout citoyen le droit d'accès aux informations touchant aux questions d'environnement. En second lieu, chaque citoyen peut participer aux processus décisionnels touchant à l'environnement; par exemple, tout un chacun serait habilité à participer aux procédures concernant la construction d'une autoroute. En troisième lieu, elle prévoit pour tout citoyen le droit à l'accès à un tribunal lorsque, par exemple, des informations importantes en matière d'environnement lui sont refusées ou que l'activité d'une autorité ou d'un particulier se heurte aux prescriptions environnementales. Aussi d'autres cantons doivent adapter leurs lois afin de garantir la conformité avec cette convention.

L'avant-projet de révision de la LInf du canton de Fribourg prévoit une proposition principale et une variante. Le canton a également invité le Préposé à participer à la consultation. La variante se limite aux adaptations paraissant absolument nécessaires; en d'autres termes, les modifications ne concerneraient ici que le domaine de l'environnement. La proposition principale par contre reprend les objets de la convention sans se limiter aux questions environnementales. Une partie des dispositions législatives proposées seraient ainsi applicables aux documents administratifs qui ne concernent pas l'environnement.

Dans sa prise de position, le Préposé s'est prononcé clairement en faveur de la proposition principale car elle conduit à une plus grande transparence des autorités par rapport à la variante. D'une part, parce qu'elle prévoit d'élargir le cercle des particuliers auprès desquels il est possible de recueillir des informations; en effet, jusqu'ici, ceux-ci devaient exercer une fonction publique (par ex. approvisionnement privé en eau) et posséder une compétence décisionnelle. Désormais,

la compétence décisionnelle devrait disparaître comme condition. D'autre part, la disposition légale qui, actuellement, soustrait des documents à l'accès du public en raison de leur date d'établissement ou de notification, est supprimée. Cela permettrait désormais l'accès à des documents qui ont été établis avant l'entrée en vigueur de la Linf.

Enfin, le Préposé a souligné la vision prospective de la proposition principale en cas d'adhésion de la Suisse à la Convention de Tromsø. Celle-ci contient des dispositions similaires à la Convention d'Aarhus qui ne s'appliquent pas seulement aux documents touchant aux questions environnementales, mais à tous les documents administratifs. Si le canton de Fribourg ne modifiait maintenant que les prescriptions en matière d'environnement, il devrait peut-être modifier celles-ci de nouveau dans quelques années en fonction de la Convention de Tromsø. En résumé, de l'avis du Préposé, il est permis de dire que le canton de Fribourg, avec cet avant-projet, donne un signe fort pour une administration ouverte et transparente.

2.4 Varia

2.4.1 Conférence internationale des commissaires à l'information 2015

84

La neuvième Conférence internationale des commissaires à l'information (ICIC International Conference of Information Commissioners) a eu lieu du 21 au 23 avril 2015 à Santiago au Chili. Organisée par le Conseil chilien pour la transparence (Consejo para la Transparencia), cette rencontre a débuté par une journée non publique de discussions, à laquelle ont participé 33 délégués de 25 pays. Elle a été suivie de deux journées de débats et de conférences ouvertes au public sur le thème de la liberté de l'information.

Au cours de la première journée, conformément à la proposition des autorités d'accueil, quatre thèmes ont été débattus et traités de manière approfondie au sein de groupes de travail. Leurs conclusions et accords, accompagnés d'une déclaration finale, ont été consignés dans une résolution commune. Les commissaires y expriment leurs préoccupations à propos des grands défis auxquels est confronté le droit d'accès à l'information. Ils y font également état des reculs de la liberté de l'information dus à l'adoption de lois et de politiques publiques plus restrictives qui

contredisent ce droit, ainsi qu'à l'absence de financement et de soutien appropriés des commissaires ou des organes de surveillance responsables.

La résolution de la neuvième ICIC peut être consultée [sur notre site Internet](#).

2.4.2 Relations avec les préposés cantonaux à la transparence

Le Préposé fédéral et les préposés cantonaux à la transparence, chargés des procédures de médiation, se rencontrent depuis 2011 une à deux fois par an pour un échange approfondi d'expériences. À la suite de plusieurs changements intervenus dans les cantons, le groupe nouvellement constitué s'est réuni en 2015. Ainsi qu'il avait été convenu en 2014, chacune de ces rencontres informelles est organisée par l'un des membres du groupe de travail. Ainsi, en 2015, ceux-ci se sont réunis à l'invitation respective des préposés à la transparence des cantons de Fribourg et de Soleure.

Il est parfois difficile de répondre aisément aux questions qui se posent dans la pratique au vu de la rareté de la jurisprudence et de la doctrine. En outre, les cantons et la Confédération possèdent une multitude de réglementations différentes en matière de protection des données et de transparence. Il est donc essentiel pour les participants au groupe de travail d'échanger leurs expériences professionnelles. D'une part, ils débattent des questions touchant les deux domaines juridiques que sont la protection des données et le principe de la transparence. D'autre part, ils se font mutuellement part de leurs expériences en matière de médiation. L'année prochaine, le groupe de travail fêtera ses cinq ans d'existence.

3. Le PFPDT

3.1 Dixième Journée de la protection des données

Fin janvier s'est tenue la 10^e édition de la Journée internationale de la protection des données, sur le thème «Cloud Computing: comment protéger les données personnelles après la décision Safe Harbor». Nous avons organisé une manifestation publique avec de courtes présentations et un débat à l'Université de Lausanne.

Les particuliers comme les entreprises utilisent de plus en plus les services du cloud, car ceux-ci offrent des avantages pratiques par rapport aux supports de stockage physiques: les données personnelles sont consultables en ligne à tout moment et peuvent être transférées en quelques clics d'un appareil à l'autre. L'espace de stockage sur Internet étant par ailleurs bon marché, de plus en plus d'entreprises et de PME helvétiques confient le traitement de leurs données à des services externes. Nous jugeons cette évolution d'un œil critique, étant donné que les données ne se trouvent plus dans le réseau interne mais qu'elles sont stockées dans un «nuage de données», souvent dans des pays offrant un niveau insuffisant de protection des données.

Depuis que la Cour de justice de l'Union européenne a invalidé l'accord Safe Harbor conclu entre l'UE et les États-Unis, les débats concernant les services de cloud se sont intensifiés, car ceux-ci sont souvent proposés à partir des États-Unis. Actuellement, le transfert de données personnelles vers les États-Unis depuis la Suisse manque à notre avis également de base juridique appropriée. Astrid Epiney, titulaire de la chaire de droit européen, droit international et droit public de l'Université de Fribourg, a évoqué dans sa présentation les problèmes actuels qui se posent en matière de droit de la protection des données. Des experts informatiques des Universités de Genève et de Lausanne ont de leur côté présenté dans une courte allocution les opportunités et les risques technologiques liés au cloud computing.

Suite aux conférences et présentations, Jean-Philippe Walter, Préposé fédéral ad interim à la protection des données et à la transparence, a discuté avec des personnalités politiques et des spécialistes informatiques lors d'une table ronde sur les risques liés à l'externalisation du traitement des données. La manifestation a attiré un large public dont les questions parfois critiques ont suscité un débat intense. Les citoyens intéressés avaient la possibilité d'exprimer leur opinion sur notre blog autour du thème «La face cachée de l'informatique en nuage (cloud computing)». Les présentations de la manifestation ainsi qu'un message vidéo de Jean-Philippe Walter sont disponibles [sur notre site Internet](#).

3.2 Publications du PFPDT durant l'exercice

Les citoyens intéressés et concernés peuvent trouver sur le site Internet du PFPDT des informations complètes sur nos thèmes et domaines de compétences: www.leprepose.ch. Durant l'exercice sous revue, nous avons publié un grand nombre de recommandations relatives à la loi sur la transparence. En matière de protection des données, de nouvelles explications ont été ajoutées concernant le contrôle de sécurité relatif aux personnes et l'héritage numérique.

Les entreprises ont un intérêt à employer des collaborateurs avec un profil de risque bas. En particulier dans les secteurs bancaires, de l'informatique, ou des technologies de pointe où les employés ont accès à des données et équipements sensibles. Dans ces cas il est de mise d'effectuer des contrôles de sécurité. Les explications qui figurent [sur notre site Internet](#) indiquent les directives que les employeurs privés devraient appliquer en matière de droit de la protection des données.

Notre vie étant de plus en plus «connectée», la quantité de données que nous stockons sur Internet sous forme de contacts, de profils personnels, de comptes d'utilisateurs, de photos, de vidéos, de tweets et de «J'aime» ne cesse d'augmenter. Afin de garantir le droit à l'autodétermination informationnelle au-delà de notre mort et de pouvoir décider de ce qu'il advient de nos données, nous devons penser suffisamment tôt à notre héritage numérique. [Nous expliquons](#) non seulement les conditions juridiques générales mais proposons également des conseils importants pour les utilisateurs d'Internet et leurs proches.

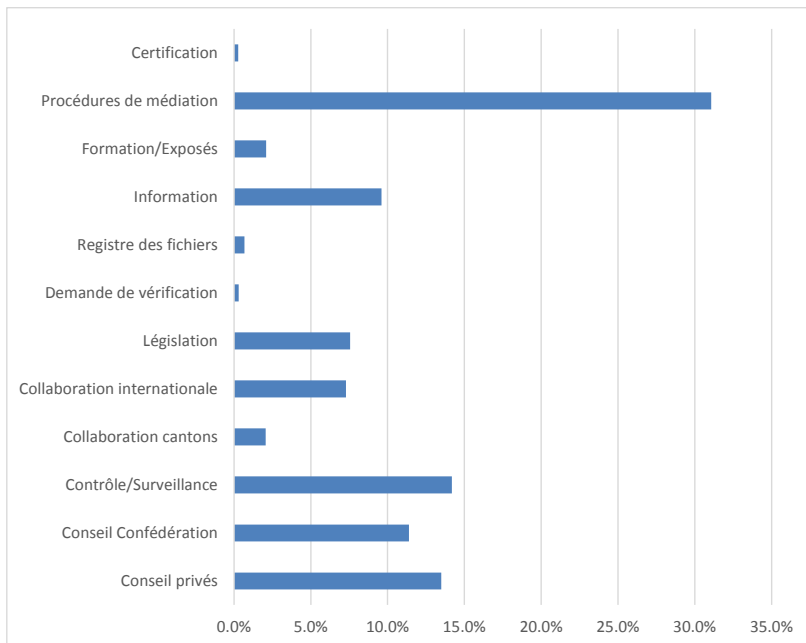
De plus en plus de compagnies d'assurance automobile évaluent les données sur le comportement de leurs clients, sous le nom «Pay as you drive» (PAYD), afin de proposer des primes de risque sur mesure. Le choix d'un tel produit (consentement) doit être libre. Toutefois, le consentement est considéré de moins en libre en cas de forts écarts de prix intervenants avec d'autres prestations qui prévoient la même couverture de risques, Le cas échéant, une contrainte économique se substitue à l'élément de liberté du consentement. Ce qui est problématique du point de vue de la protection des données. Nous avons donc actualisé [nos commentaires](#) relatifs aux modèles de primes d'assurance basés sur le risque.

Suite à l'arrêt rendu par la Cour de justice de l'Union européenne concernant l'accord [Safe Harbor](#), le PFPDT a rédigé une prise de position et actualisé ses remarques sur la transmission de données aux États-Unis. Jusqu'à ce qu'un nouvel accord soit négocié avec les États-Unis, nous recommandons de convenir de garanties contractuelles au sens de la LPD pour l'échange de données avec des entreprises américaines. Bien que cette démarche n'exclut pas un accès aux données par les autorités américaines, elle permet d'assurer un meilleur niveau de protection.

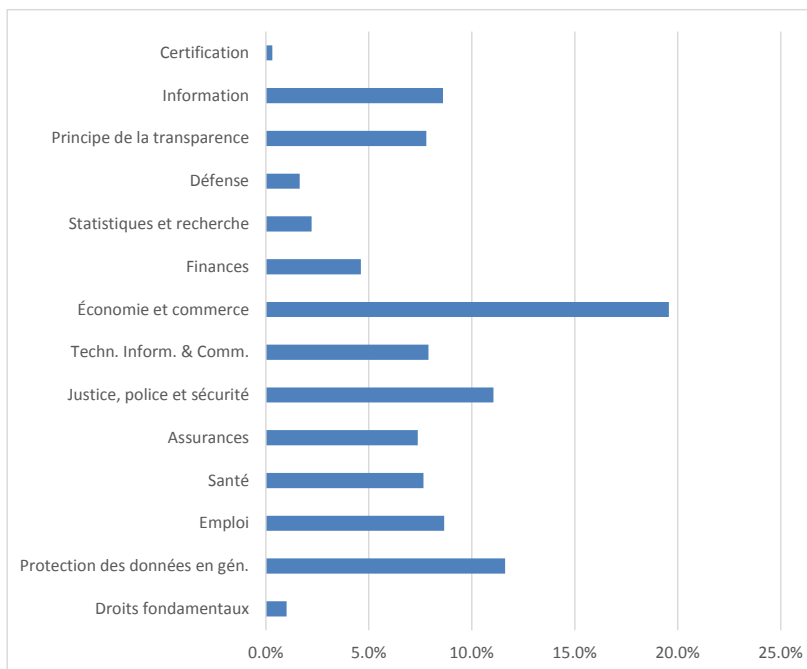
L'Office fédéral de la communication (OFCOM) a mis en ligne avec le PFPDT et d'autres partenaires le site Internet «Petites histoires d'Internet», qui présente 15 histoires en bande dessinée sur les expériences d'une famille avec Internet, afin de sensibiliser notamment les jeunes à la nécessité d'adopter un comportement raisonnable et sûr lors de l'utilisation des technologies de l'information et de la communication (TIC). Les bandes dessinées [publiées sur Internet](#) peuvent également être commandées gratuitement sous forme de brochures.

3.3 Statistique des activités du PFPDT du 1^{er} avril 2015 au 31 mars 2016

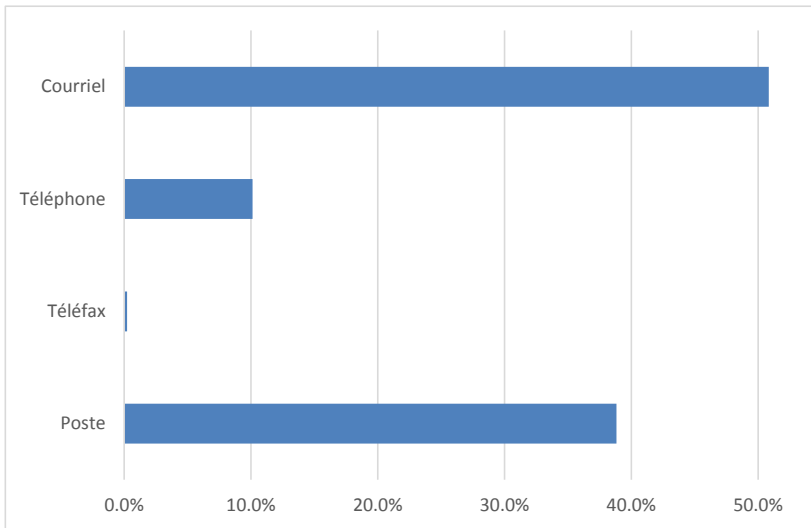
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.4 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1^{er} janvier 2015 au 31 décembre 2015)

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
ChF	17	7	4	3	3	0
DFAE	134	110	7	17	0	0
DFI	77	23	10	28	4	12
DFJP	46	16	13	13	3	1
DDPS	63	20	22	12	6	3
DFF	84	53	20	11	0	0
DEFR	75	34	9	22	4	6
DETEC	101	56	13	21	2	9
Total 2015 (en %)	597 (100 %)	319 (54 %)	98 (16 %)	127 (21 %)	22 (4 %)	31 (5 %)
Total 2014 (en %)	575 (100 %)	297 (51 %)	122 (21 %)	124 (22 %)	17 (3 %)	15 (3 %)
Total 2013 (en %)	469 (100 %)	218 (46 %)	122 (26 %)	103 (22 %)	8 (2 %)	18 (4 %)
Total 2012 (en %)	506 (100 %)	223 (44 %)	138 (27 %)	120 (24 %)	6 (1 %)	19 (4 %)
Total 2011 (en %)	466 (100 %)	203 (44 %)	126 (27 %)	128 (27 %)	9 (2 %)	-
Total 2010 (en %)	239 (100 %)	106 (45 %)	62 (26 %)	63 (26 %)	8 (3 %)	-
Total 2009 (en %)	232 (100 %)	124 (54 %)	68 (29 %)	40 (17 %)	-	-

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
BK	10	1	4	2	3	0
PPPDT	7	6	0	1	0	0
Total	17	7	4	3	3	0

Département fédéral des affaires étrangères DFAE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
DFAE	134	110	7	17	0	0
Total	134	110	7	17	0	0

Département fédéral de l'intérieur DFI

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	3	1	0	1	0	1
BFEG	0	0	0	0	0	0
OFC	1	1	0	0	0	0
AFS	6	6	0	0	0	0
METEO CH	0	0	0	0	0	0
BN	0	0	0	0	0	0
OFSP	22	3	4	11	2	2
OFS	4	0	0	2	0	2
OFAS	21	10	0	10	1	0
OSAV	4	1	0	2	0	1
MNS	0	0	0	0	0	0
SWISS-MEDIC	13	0	4	2	1	6
SUVA	3	1	2	0	0	0
Total	77	23	10	28	4	12

Département fédéral de justice et police DFJP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	9	5	0	1	3	0
OFJ	2	0	2	0	0	0
FEDPOL	6	2	3	1	0	0
METAS	2	1	0	1	0	0
ODM	19	3	6	9	0	1
ISDC	5	3	1	1	0	0
IPI	2	2	0	0	0	0
CFMJ	0	0	0	0	0	0
CAF	0	0	0	0	0	0
ASR	0	0	0	0	0	0
CSI	1	0	1	0	0	0
CNPT	0	0	0	0	0	0
Total	46	16	13	13	3	1

**Département fédéral de la défense, de la protection
de la population et des sports DDPS**

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	22	13	4	4	1	0
Défense/ armée	16	4	7	2	3	0
SRC	15	0	7	6	1	1
arma- suisse	8	1	4	0	1	2
OFSPD	2	2	0	0	0	0
OFPP	0	0	0	0	0	0
Total	63	20	22	12	6	3

Département fédéral des finances DFF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	18	10	6	2	0	0
UPIC	4	2	0	2	0	0
AFF	1	0	0	1	0	0
OFFER	1	0	1	0	0	0
AFC	5	0	5	0	0	0
AFD	3	1	1	1	0	0
RFA	4	0	1	3	0	0
OFCL	1	0	0	1	0	0
OFIT	2	1	0	1	0	0
CDF	43	39	4	0	0	0
SFI	1	0	1	0	0	0
PUBLICA	0	0	0	0	0	0
CdC	1	0	1	0	0	0
Total	84	53	20	11	0	0

Département fédéral de l'économie, de la formation et de la recherche DEFR

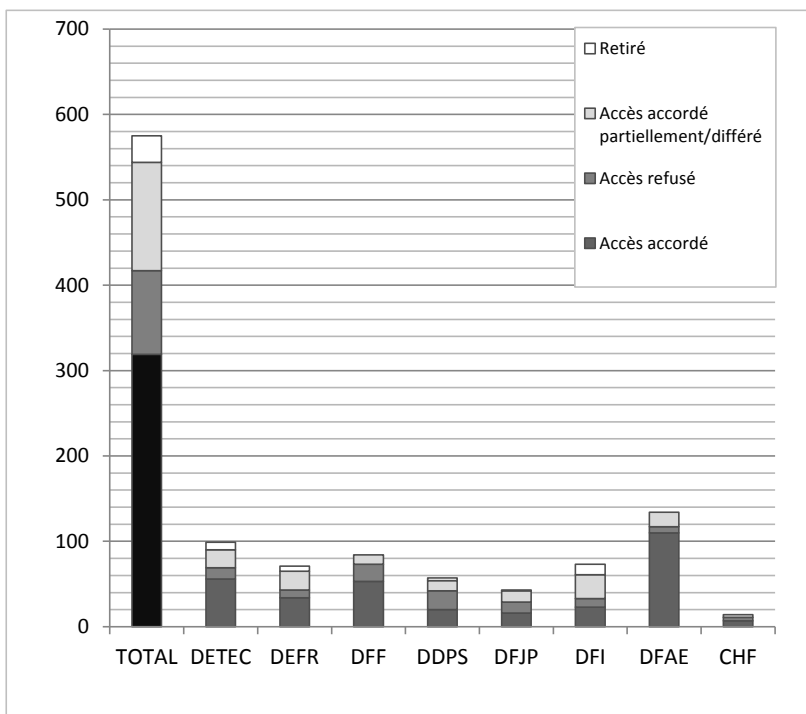
Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	6	1	2	0	3	0
SECO	6	1	2	3	0	0
SEFRI	4	1	1	1	0	1
OFAG	23	13	1	9	0	0
OFAE	0	0	0	0	0	0
OFL	0	0	0	0	0	0
SPr	2	0	2	0	0	0
COMCO	23	14	1	3	1	4
ZIVI	0	0	0	0	0	0
BFC	1	1	0	0	0	0
FNS	0	0	0	0	0	0
IFFP	0	0	0	0	0	0
CEPF	10	3	0	6	0	1
Total	75	34	9	22	4	6

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SG	6	3	1	0	2	0
OFT	5	2	0	0	0	3
OFAC	6	2	2	2	0	0
OFEN	13	7	4	1	0	1
OFROU	4	1	1	1	0	1
OFCOM	11	2	1	4	0	4
OFEV	31	26	1	4	0	0
ARE	4	4	0	0	0	0
ComCom	0	0	0	0	0	0
IFSN	17	5	3	9	0	0
PostCom	0	0	0	0	0	0
AIEP	4	4	0	0	0	0
Total	101	56	13	21	2	9

Traitement des demandes d'accès

23^e Rapport d'activités 2015/2016 du PFPDT
100



3.5 Statistique des demandes d'accès présentées auprès du Ministère public de la Confédération en vertu de l'art. 6 de la loi sur la transparence (Période: 1^{er} janvier 2015 au 31 décembre 2015)

Ministère public de la Confédération MPC

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
MPC	1	0	0	1	0	0
Total	1	0	0	1	0	0

3.6 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période: 1^{er} janvier 2015 au 31 décembre 2015)

Services du Parlement SP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante	Demande d'accès retiré
SP	2	1	1	0	0	0
Total	2	1	1	0	0	0

3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1^{er} janvier 2015 au 31 décembre 2015)

Catégorie de requérants	2015
Médias	26
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	23
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	14
Avocats	14
Entreprises	21
Total	98

3.8 Secrétariat du PFPDT

Préposé fédéral à la protection des données et à la transparence:

Jusqu'au 30 novembre 2015: Thür Hanspeter

À partir du 1^{er} décembre 2015: Walter Jean-Philippe

Secrétariat:

Chef: Walter Jean-Philippe

Suppléant: Buntschu Marc

Unité 1: 11

Unité 2: 14

Unité 3: 5 (dont 1 stagiaire)

Chancellerie: 2

4. Liste des abréviations

AFC	Administration fédérale des contributions
AFD	Administration fédérale des douanes
AFF	Administration fédérale des finances
AFS	Archives fédérales suisses
AIEP	Autorité indépendante d'examen des plaintes en matière de radio-télévision
ARE	Office fédéral du développement territorial
armasuisse	Office fédéral de l'armement
ASR	Autorité fédérale de surveillance en matière de révision
BFC	Bureau fédéral de la consommation
BFEG	Bureau fédéral de l'égalité entre femmes et hommes
BN	Bibliothèque nationale suisse
CAF	Commission arbitrale fédérale pour la gestion de droits d'auteur et de droits voisins
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CFMJ	Commission fédérale des maisons de jeu
CNPT	Commission nationale de prévention de la torture
COMCO	Commission de la concurrence
ComCom	Commission fédérale de la communication
CSI	Centre de services informatiques
fedpol	Office fédéral de la police
FNS	Fonds national suisse
IFFP	Institut fédéral des hautes études en formation professionnelle
IFSN	Inspection fédérale de la sécurité nucléaire
IPI	Institut fédéral de la propriété intellectuelle
ISDC	Institut suisse de droit comparé
METEO CH	Office fédéral de météorologie et de climatologie
OFAC	Office fédéral de l'aviation civile
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales

OFC	Office fédéral de la culture
OFCL	Office fédéral des constructions et de la logistique
OFCOM	Office fédéral de la communication
OFEN	Office fédéral de l'énergie
OFEV	Office fédéral de l'environnement
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFL	Office fédéral du logement
OFPER	Office fédéral du personnel
OFPP	Office fédéral de la protection de la population
OFROU	Office fédéral des routes
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFSP0	Office fédéral du sport
OFT	Office fédéral des transports
OSAV	Office fédéral de la sécurité alimentaire et des affaires vétérinaires
PostCom	Commission fédérale de la poste
PUBLICA	Caisse fédérale de pensions
METAS	Office fédéral de métrologie
MNS	Musée national suisse
RFA	Régie fédérale des alcools
SECO	Secrétariat d'État à l'économie
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
SEM	Secrétariat d'État aux migrations
SFI	Secrétariat d'État aux questions financières internationales
SPR	Surveillant des prix
SUVA	Caisse nationale suisse d'assurance en cas d'accidents (CNA)
SWISSMEDIC	Institut suisse des produits thérapeutiques
UPIC	Unité de pilotage informatique de la Confédération
ZIVI	Organe d'exécution du service civil