Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.059

Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales

du 15 septembre 2017

Messieurs les Présidents,
Mesdames, Messieurs,

Par le présent message, nous soumettons à votre approbation la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, ainsi que l'arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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.

Nous vous proposons simultanément de classer les interventions parlementaires suivantes:

- Postulat Hodgers 10.3383 «Adapter la loi sur la protection des données aux nouvelles technologies»;
- Postulat Graber 10.3651 «Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles»;
- Postulat Schwaab 12.3152 «Droit à l'oubli numérique»;
- Postulat Recordon 13.3989 «Violations de la personnalité dues au progrès des techniques de l'information et de la communication»;
- Motion Comte 14.3288 «Faire de l'usurpation d'identité une infraction pénale en tant que telle»;
- Postulat Derder 14.3655 «Définir notre identité numérique et identifier les solutions pour la protéger»;
- Postulat Schwaab 14.3739 «Control by design. Renforcer les droits de propriété pour empêcher les connexions indésirables»;
- Postulat Groupe libéral-radical 14.4137 «Enregistrements vidéo par des privés. Mieux protéger la sphère privée»;

– Postulat Comte 14.4284 «Enregistrements vidéo par des privés. Mieux protéger la sphère privée»;
– Postulat Béglé 16.3383 «Données numériques. Informer les personnes lésées en cas de piratage»;
– Postulat Béglé 16.3384 «Données numériques médicales. Assurer une collecte protégée, transparente et ciblée dans la révision de la loi sur la protection des données».

Nous vous prions d'agréer, Messieurs les Présidents, Mesdames, Messieurs, l'assurance de notre haute considération.

15 septembre 2017

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Doris Leuthard
Le chancelier de la Confédération, Walter Thurnherr

Condensé

Le présent projet de loi vise à renforcer la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle que les personnes concernées peuvent exercer sur leurs données. Le projet a également pour objectif de responsabiliser les responsables du traitement en les incitant notamment à prendre en considération les enjeux de protection des données dès la mise en place de nouveaux traitements. Il vise de plus à renforcer la surveillance de l'application et du respect des dispositions fédérales de protection des données. Enfin, il a pour but de maintenir et de renforcer la compétitivité de la Suisse en créant un environnement propre à faciliter les flux transfrontières de données et en favorisant l'émergence de nouvelles activités économiques en lien avec la société numérique, ce qui passe par un standard de protection élevé, reconnu au plan international.

Contexte et buts du projet

Le présent projet vise à réaliser deux objectifs principaux: renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies d'une part, et d'autre part tenir compte des réformes du Conseil de l'Europe et de l'Union européenne en la matière. L'avant-projet a été mis en consultation externe du 21 décembre 2016 au 4 avril 2017.

Le 27 avril 2016, l'Union européenne a adopté une réforme de sa législation sur la protection des données qui comprend deux actes législatifs. Il s'agit d'une part du règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Le second acte adopté est la directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel à des fins pénales. Seule celle-ci est considérée comme un développement de l'acquis de Schengen. Au niveau du Conseil de l'Europe, un protocole d'amendement de la convention STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel doit encore être adopté par le Comité des Ministres

Le projet vise à rendre la législation fédérale compatible avec la convention STE 108 modernisée. En effet, il est dans l'intérêt de la Suisse d'approuver le projet d'amendement de cet instrument dès qu'il sera ouvert à la signature. Le présent projet a également pour objectif de mettre en œuvre les exigences de la directive (UE) 2016/680, conformément aux engagements pris par la Suisse dans le cadre de l'accord d'association à Schengen. La révision met en outre en œuvre les recommandations faites par l'Union européenne lors de l'évaluation de la Suisse dans le cadre de l'accord d'association à Schengen, selon lesquelles les pouvoirs du Préposé fédéral à la protection des données et à la transparence (préposé) devraient être renforcés. Enfin, le projet doit permettre de rapprocher le droit fédéral des exigences du règlement (UE) 2016/679. Ce rapprochement, ainsi que l'approbation de la future convention STE 108, constituent, de l'avis du Conseil fédéral, des conditions déterminantes pour que la Commission européenne maintienne la décision

d'adéquation accordée à la Suisse et selon laquelle cette dernière offre un niveau de protection des données adéquat. Cette décision a une importance centrale surtout pour l'économie suisse.

L'adoption du message relatif au projet figure parmi les objectifs du Conseil fédéral de 2017 et dans le programme de la législature 2015 à 2019. La révision de la protection des données a également fait l'objet de nombreuses interventions parlementaires ces dernières années, montrant ainsi l'existence d'une volonté politique de renforcer la législation fédérale dans ce domaine.

Contenu du projet

Le projet comprend tout d'abord une révision totale de la loi fédérale sur la protection des données.

La révision renonce à la protection des données des personnes morales, en adéquation avec les règles européennes de protection des données et la majorité des législations étrangères. Cette mesure facilite notamment les échanges de données avec l'étranger.

La transparence des traitements est améliorée: le devoir d'information lors de la collecte est étendu à tous les traitements dans le secteur privé. Il est assorti d'exceptions et peut être rempli de manière standardisée. La révision introduit en outre un devoir spécifique d'information lors de décisions individuelles automatisées ainsi que le droit pour la personne concernée, à certaines conditions, de faire valoir son point de vue et de demander que la décision soit revue par une personne physique. Elle étend également les informations à fournir à la personne concernée lorsque celle-ci exerce son droit d'accès.

La révision encourage le développement de l'autoréglementation, par le biais de codes de conduite qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Ces codes sont élaborés par les branches et peuvent être soumis au préposé.

Le statut et l'indépendance du préposé sont renforcés. La révision prévoit que celui-ci peut prendre, à l'instar de ses homologues européens, des décisions contraignantes à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur dénonciation.

Le volet pénal de la loi est renforcé à plusieurs égards, pour compenser notamment le fait que le préposé, contrairement à la quasi-totalité de ses homologues européens, n'a pas le pouvoir d'infliger des sanctions administratives.

En sus de la révision totale de la loi fédérale sur la protection des données, le projet comprend également une révision partielle d'autres lois fédérales, notamment afin de mettre en œuvre les exigences de la directive (UE) 2016/680. Il s'agit principalement du code pénal, du code de procédure pénale, de la loi sur l'entraide pénale internationale et de la loi sur l'échange d'information Schengen.

Table des matières

Message

1 Présentation du projet

1.1 Contexte national

1.1.1 Droit en vigueur

La protection des données est actuellement régie, au niveau fédéral, par la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[1], qui est entrée en vigueur le 1er juillet 1993.

La LPD règle le traitement de données concernant des personnes physiques et des personnes morales effectué par des personnes privées et des organes fédéraux (art. 2, al. 1). Cette loi ne s'applique toutefois pas aux données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers (al. 2, let. a), aux délibérations des Chambres fédérales et des commissions parlementaires (al. 2, let. b), aux procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif, à l'exception des procédures administratives de première instance (al. 2, let. c), aux registres publics relatifs aux rapports juridiques de droit privé (al. 2, let. d) et enfin aux données personnelles traitées par le Comité international de la Croix-Rouge (CICR) (al. 2, let. e).

La LPD fixe les principes à respecter lors du traitement de données. Elle prescrit en particulier que tout traitement de données personnelles doit être licite (art. 4, al. 1), respecter les principes de la bonne foi et de la proportionnalité (art. 4, al. 2) et être effectué uniquement dans le but qui est indiqué lors de la collecte des données, qui est prévu par une loi ou qui ressort des circonstances (art. 4, al. 3). La collecte de données, et en particulier la finalité du traitement, doivent en outre être reconnaissables pour la personne concernée (art. 4, al. 4). L'art. 4, al. 5, détermine quant à lui les conditions applicables au consentement de la personne concernée. D'autre part, la personne privée ou l'organe fédéral qui traite des données personnelles doit s'assurer qu'elles sont correctes (art. 5).

La LPD règle la communication des données à l'étranger (art. 6), de même que le droit d'accès (art. 8 à 10). L'art. 10*a* régit le traitement de données par un tiers. L'art. 11*a* prévoit une obligation pour le Préposé fédéral à la protection des données et à la transparence (préposé) de tenir un registre des fichiers en ligne et accessible au public ainsi qu'un devoir pour les maîtres du fichier de déclarer leurs fichiers sous réserve d'exceptions.

La section 3 contient des dispositions applicables aux traitements de données effectués dans le secteur privé. Ainsi, la LPD interdit aux personnes privées qui traitent des données personnelles de porter une atteinte illicite à la personnalité des personnes concernées (art. 12, al. 1) et en particulier de traiter des données contre la volonté expresse de la personne concernée en l'absence de motif justificatif (art. 12,

[1] RS **235.1**

al. 2, let. b, et art. 13). L'art. 14 prévoit une obligation pour les personnes privées d'informer la personne concernée de toute collecte de données sensibles ou de profils de la personnalité les concernant, sous réserve d'exceptions. Cette section règle en outre les prétentions de droit civil que les personnes lésées peuvent faire valoir, ainsi que la procédure applicable (art. 15).

Les art. 16 à 25 LPD régissent le traitement de données personnelles par des organes fédéraux. Ceux-ci ne sont en droit de traiter des données personnelles que s'il existe une base légale (art. 17, al. 1). Une base légale dans une loi au sens formel est exigée pour le traitement de données sensibles ou de profils de la personnalité (art. 17, al. 2). L'art. 18*a* prévoit une obligation pour les organes fédéraux d'informer la personne concernée de toute collecte de données personnelles la concernant, sous réserve de certaines exceptions (art. 18*b*). La communication de données personnelles à des tiers est subordonnée en principe à l'existence d'une base légale (art. 19, al. 1). Les données personnelles ne peuvent être rendues accessibles au moyen d'une procédure d'appel que si cela est prévu expressément par la loi (art. 19, al. 3). Les exigences sont encore plus strictes pour les données sensibles ou les profils de la personnalité, lesquels ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément (art. 19, al. 3). Quant à l'art. 25, il règle les prétentions que les personnes concernées peuvent faire valoir à l'encontre d'un organe fédéral responsable d'un traitement les concernant.

La LPD règle aux art. 26 et 26*a* la procédure de nomination, le statut, le renouvellement et la fin des rapports de fonction du préposé. Les art. 27 à 33 définissent les tâches et les compétences du préposé. Celui-ci surveille l'application de la loi par les organes fédéraux et conseille les personnes privées. Il a la compétence d'effectuer des enquêtes et peut émettre des recommandations. Lorsqu'une recommandation n'est pas suivie par une personne privée, il peut porter l'affaire devant le Tribunal administratif fédéral pour décision et a qualité pour recourir contre cette décision (art. 29, al. 4). Dans le secteur public, il peut porter l'affaire pour décision auprès du département ou de la Chancellerie fédérale (art. 27, al. 5). Il peut recourir contre la décision de l'autorité supérieure ainsi que contre celle de l'autorité de recours (art. 27, al. 6).

La LPD prévoit enfin des dispositions pénales aux art. 34 et 35 en cas de violation des obligations de renseigner, de déclarer et de collaborer ainsi qu'en cas de violation du devoir de discrétion.

Les traitements de données effectués par des organes cantonaux (ou communaux) relèvent – sous réserve de l'art. 37 LPD ou de règles contenues dans des lois fédérales spéciales – du droit cantonal, y compris lorsque les organes en question exécutent le droit fédéral ou ont obtenu les données au moyen d'un accès en ligne à une banque de données fédérale.

Enfin, d'autres lois fédérales que la LPD contiennent des dispositions spéciales de protection des données qui s'appliquent dans de nombreux domaines.

1.1.2 Travaux préparatoires et concept

Durant les années 2010 et 2011, la LPD a fait l'objet d'une évaluation[2]. Il en est ressorti que les développements technologiques et sociétaux intervenus depuis son entrée en vigueur avaient entraîné de nouvelles menaces pour la protection des données et que la loi ne suffit plus, dans certains contextes, à garantir une protection suffisante. Se fondant sur les conclusions de l'évaluation et sur son rapport du 9 décembre 2011[3], le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'examiner des mesures législatives permettant de renforcer la protection des données afin de prendre en compte les nouvelles menaces qui pèsent sur la sphère privée.

Pour donner suite au mandat du Conseil fédéral du 9 décembre 2011, l'Office fédéral de la justice (OFJ) a mis sur pied un groupe de travail chargé d'accompagner les travaux de révision de la LPD. Il était composé de représentants de l'administration fédérale[4], des cantons[5], des milieux économiques[6], des associations de protection des consommateurs[7] ainsi que d'experts. Les réflexions du groupe d'accompagnement sont présentées dans un rapport du 29 octobre 2014 intitulé «Esquisse d'acte normatif relative à la révision de la loi sur la protection des données»[8].

Le 1er avril 2015, le Conseil fédéral a pris acte du rapport susmentionné et a chargé le DFJP d'élaborer, en collaboration avec le préposé, le Département fédéral de l'économie, de la formation et de la recherche (DEFR), le Département fédéral des finances (DFF) et le Département fédéral de l'intérieur (DFI), un avant-projet de loi, qui tienne compte des conclusions dudit rapport et des réformes du Conseil de l'Europe et de l'Union européenne.

L'avant-projet a été mis en consultation externe le 21 décembre 2016. La consultation a porté sur trois objets. Premièrement un avant-projet de loi, soit un acte modificateur unique intitulé «Avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales». Il réunissait sous un même titre une révision totale de la LPD (AP-LPD) et la révision partielle d'autres lois de même niveau. Deuxièmement, le projet d'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'Union euro-

2 Büro Vatter/Institut für Europarecht, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Berne, 10 mars 2011. www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf.

3 Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF **2012** 255.

4 Les autorités fédérales suivantes étaient représentées: l'Office fédéral de la justice (OFJ; conduite du projet), le préposé, la Chancellerie fédérale (ChF), l'Office fédéral de la communication (OFCOM), les Archives fédérales suisses (AFS), le Bureau fédéral de la consommation (BFC), le Secrétariat général du Département fédéral de justice et police (SG_DFJP).

5 Les cantons étaient représentés par l'association des commissaires suisses à la protection des données (PRIVATIM).

6 Les milieux économiques étaient représentés par economiesuisse et par l'Union suisse des arts et métiers (USAM).

7 Les associations de protection des consommateurs étaient représentées par la Fédération romande des consommateurs.

8 www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf

péenne (UE) sur la reprise de la directive (UE) 2016/680. Troisièmement, le projet de modernisation de la convention du Conseil de l'Europe STE 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (P-STE 108).

L'avant-projet avait en particulier pour objectif de:

- transposer les exigences de la directive (UE) 2016/680[9] (cf. ch. 2);
- mettre en œuvre les recommandations reçues dans le cadre de l'évaluation Schengen de 2014 (cf. ch. 1.2.2.3);
- rapprocher la LPD des exigences du règlement (UE) 2016/679[10] (cf. ch. 4);
- reprendre les exigences du P-STE 108 (cf. ch. 3).

La procédure de consultation s'est terminée le 4 avril 2017.

Sur la base des résultats de la consultation externe, le Conseil fédéral a élaboré un projet de loi. La forme est la même que l'avant-projet, à savoir un acte modificateur unique sujet au référendum (projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales; ci-après «projet de loi»). Le chiffre I de l'acte modificateur unique comprend la révision totale de la LPD («P-LPD») et, dans l'annexe, les modifications d'autres lois fédérales rendues nécessaires par la révision de la LPD. Le chiffre II de l'acte modificateur unique comprend la modification d'autres lois fédérales en lien avec la transposition de la directive (UE) 2016/680 conformément aux engagements pris par la Suisse dans le cadre de l'accord d'association du 26 octobre 2004 conclu entre la Confédération, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (accord d'association à Schengen, AAS)[11]. Les actes législatifs modifiés sont désignés dans le présent rapport, par «P», suivi de l'abréviation de la loi concernée (cf. ch. 9.2 et 9.3).

1.1.3 Stratégie «Suisse numérique»

Le 20 avril 2016, le Conseil fédéral a adopté la stratégie «Suisse numérique»[12], qui a remplacé la stratégie du Conseil fédéral pour une société de l'information en Suisse, du 9 mars 2012.

9 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

10 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, JO L 119 du 4.5.2016, p. 1.

11 RS **0.362.31**

12 www.ofcm.admin.ch > Suisse numérique et internet > Stratégie Suisse numérique

Cette nouvelle stratégie vise à ce que la Suisse profite davantage de la numérisation croissante et se développe de manière encore plus dynamique en tant qu'économie novatrice. Dans ce cadre, elle entend notamment développer une politique des données cohérente et tournée vers l'avenir, qui doit permettre à la Suisse d'exploiter pleinement le potentiel de l'accroissement de la collecte et du traitement des données, sans perdre le contrôle sur ces dernières. La nouvelle stratégie «Suisse numérique» se veut une stratégie faîtière, qui coordonne les nombreuses activités en cours et les groupes d'experts existants. Cette coordination est assurée par le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC). Pour réaliser cette stratégie, un plan d'action[13], qui comprend les mesures que l'administration fédérale doit mettre en œuvre, a été mis en place. Le projet de loi fait partie d'une de ces mesures (ch. 1.2 et 1.7 du plan d'action).

Dans le cadre de la politique des données qu'il entend développer, le Conseil fédéral a donné mandat au DFJP d'examiner plusieurs questions juridiques ayant trait à la réutilisation des données numériques. A cette occasion, le DFJP examinera, entre autres, l'opportunité d'introduire un droit à la portabilité des données personnelles dans l'ordre juridique suisse. Il procédera également à une étude portant sur les possibilités offertes à la Confédération, sur la base des lois existantes et des projets de lois en cours, de réutiliser des données personnelles dans un but d'intérêt public (par ex. la statistique publique). Le DFJP doit soumettre les résultats de son travail au Conseil fédéral à la fin de l'année 2017.

Dans le cadre de l'élaboration de cette stratégie, l'Office fédéral de la communication (OFCOM) a fait réaliser une étude sur la problématique du *Big Data* (mégadonnées) par la Haute école bernoise, intitulée «Big Data: atouts, risques et mesures nécessaires pour la Confédération»[14]. Les experts arrivent en partie aux mêmes conclusions que l'évaluation de la LPD, à savoir qu'une intervention du législateur est nécessaire. Selon cette étude, il s'agit d'améliorer le fonctionnement du marché en donnant davantage de pouvoirs aux utilisateurs et en renforçant la réglementation et le contrôle des acteurs privés par l'Etat. Les mesures prévues par le projet de loi vont dans ce sens.

1.1.4 Autres projets de l'administration fédérale en lien avec la protection des données

Au sein de l'administration fédérale, de nombreux projets concernent la protection des données. Parmi les projets en cours, on peut citer les suivants, qui sont les plus importants:

13 www.bakom.admin.ch/dam/bakom/fr/dokumente/informationsgesellschaft/strategie/aktionsplan_digitale_schweiz.pdf.download.pdf/aktionsplan_digitale_schweiz_FR.pdf

14 «Big Data: atouts, risques et mesures nécessaires pour la Confédération», disponible (en allemand uniquement) sous: www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/big-data.html.

Stratégie nationale de protection de la Suisse contre les cyberrisques, du 27 juin 2012 (SNPC)[15]: cette stratégie concerne la protection des infrastructures utilisant les technologies de l'information et de la communication contre les cyberrisques. Elle vise à détecter de manière précoce les menaces dans le cyberespace, à renforcer la capacité de résistance des infrastructures d'importance vitale et à réduire les cyberrisques liés en particulier au cyberespionnage et au cybersabotage. Sa mise en œuvre relève de la compétence du DFF. La mise en œuvre de la stratégie s'achèvera cette année conformément au calendrier prévu. Le rapport annuel 2016 sur l'état de la mise en œuvre de la SNPC, qui a été adopté le 26 avril 2017[16] par le Conseil fédéral, montre que 15 des 16 mesures prévues sont déjà réalisées. En raison de l'augmentation des cyberrisques, le Conseil fédéral a décidé de faire élaborer une deuxième stratégie pour les années 2018 à 2023, qui réponde aux menaces actuelles et tienne compte des résultats de l'évaluation de l'efficacité de la SNPC.

Stratégie Open Government Data, du 16 avril 2014 [17]: la stratégie vise à promouvoir la publication des données collectées par l'administration en tant qu'*Open Government Data* (OGD), c'est-à-dire en tant que données d'administrations publiques librement réutilisables. Même s'il s'agit généralement de publier des données agrégées et préalablement anonymisées dans la perspective de leur réutilisation, il n'en demeure pas moins que les principes de la protection des données restent applicables.

Le Programme national de recherche 75 «Big Data» (PNR 75)[18]: ce programme, doté d'un budget de 25 millions de francs, a été lancé par le Conseil fédéral en 2015. Il vise à fournir les bases scientifiques d'une utilisation efficace et adéquate des mégadonnées. Il s'articule autour de trois axes: un module sur les technologies de l'information et les services de gestion des données ainsi que les questions de sécurité, d'accès, de surveillance et de confiance; un module sur les défis sociétaux que représente le «*Big Data*» et un module sur le développement d'applications des mégadonnées dans différents domaines de la société. 35 projets de recherche ont été lancés depuis début 2017. Ils ont chacun une durée de 24 à 48 mois. Les premiers résultats seront disponibles à partir de 2019. Le programme va organiser de nombreuses activités de transfert de connaissances jusqu'en 2022.

Groupe d'experts «Avenir du traitement et de la sécurité des données»: ce groupe d'experts a été constitué par le DFF suite à l'adoption de la motion Rechsteiner 13.3841 «Commission d'experts pour l'avenir du traitement et de la sécurité des données». Le cas échéant, les travaux du groupe d'experts peuvent déboucher sur des réformes supplémentaires dans le domaine de la protection des données, bien qu'en raison du contexte européen, la marge de manœuvre du législateur suisse soit limitée. Ces besoins de réforme supplémentaires, s'ils devaient être avérés, pourraient être pris en compte lors d'une étape ultérieure. Il n'est d'ailleurs pas exclu que ces besoins de réforme concernent d'autres domaines que la protection des données

15 www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
16 www.newsd.admin.ch/newsd/message/attachments/48042.pdf
17 www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html
18 www.nfp75.ch/fr

(par ex. le code des obligations [CO][19], le droit de la propriété intellectuelle, la sécurité des objets, le droit de la concurrence, etc.). Les travaux de la commission susmentionnée ne devraient pas se terminer avant mi-2018.

Jeunes et médias – protection des enfants et des jeunes face aux médias numériques: en adoptant, le 13 mai 2015, le rapport «Jeunes et médias. Aménagement de la protection des enfants et des jeunes face aux médias en Suisse», le Conseil fédéral a décidé de poursuivre les activités initiées dans le cadre du programme national «Jeunes et médias»[20] mis en œuvre de 2011 à 2015. Le DFI (Office fédéral des assurances sociales; OFAS) est ainsi chargé de mettre en œuvre et de coordonner des activités d'ordre éducatif et réglementaire. La protection des données fait partie des thèmes abordés dans le cadre du volet éducatif.

Rapport du Conseil fédéral du 11 janvier 2017 sur les conditions-cadres pour une économie numérique[21]: le rapport traite de différents domaines qui ont une importance déterminante pour l'économie numérique. Cinq domaines ont été examinés: le marché du travail, la recherche et le développement, l'économie de partage, la finance numérique et la politique de la concurrence. Le Conseil fédéral a chargé le Secrétariat d'Etat à l'économie (SECO) d'analyser la pertinence en matière numérique des lois existantes et économiquement importantes, et de présenter l'éventuelle nécessité d'une révision, le tout basé sur un sondage auprès d'associations, de partenaires sociaux et de plusieurs entreprises sélectionnées («test numérique»). L'accent est mis sur l'identification des réglementations qui ont en grande partie perdu de leur utilité suite à l'évolution technologique.

Programmes nationaux de recherche (PNR) «Mutation numérique de l'économie et de la société»[22]: le 5 juillet 2017, le Conseil fédéral a chargé le Département fédéral de l'économie, de la formation et de la recherche (DEFR), et plus précisément le Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI), d'étudier le lancement d'une série de PNR consacrés à la thématique de la «Mutation numérique de l'économie et de la société». En association avec les cantons, il s'agit d'examiner les effets de la digitalisation sur le domaine de la formation. Il s'agit aussi d'examiner s'il y a lieu de combler certaines lacunes dans la recherche des hautes écoles. Une attention particulière doit être portée sur l'envergure que les capacités de recherche en Suisse doivent atteindre pour pouvoir assurer le transfert des connaissances et des technologies vers l'économie et garantir un fonctionnement sûr des infrastructures.

1.1.5 Interventions parlementaires

La protection des données a fait l'objet de nombreuses interventions. Seules les plus importantes sont mentionnées ci-après:

19 RS **210**
20 www.jeunesetmedias.ch/fr/accueil.html
21 www.seco.admin.ch/seco/fr/home/wirtschaftslage---wirtschaftspolitik/wirschaftspolitik/digitalisierung.html
22 www.sbfi.admin.ch/sbfi/fr/home/themes/la-recherche-et-linnovation-en-suisse/instruments-d_encouragement/programmes-nationaux-de-recherche-pnr.html

– Initiative parlementaire Vischer 14.413 «Droit fondamental à l'autodétermination en matière d'information». Selon son auteur, l'art. 13, al. 2, de la Constitution (Cst.)[23] protège toute personne uniquement «contre l'emploi abusif des données qui la concernent». Il en résulterait que le «fardeau de la preuve de l'abus incombe au citoyen et non à l'Etat ou à l'exploitant d'Internet». L'initiative vise ainsi à modifier l'art. 13, al. 2, Cst. de sorte que la garantie ne confère pas seulement un droit à la protection contre les abus mais un droit fondamental à l'autodétermination. La Commission des institutions politiques du Conseil national a accepté de donner suite à l'initiative le 29 août 2014, celle du Conseil des Etats le 20 août 2015.

– Initiative parlementaire Derder 14.434 «Protéger l'identité numérique des citoyens». L'initiative tend à modifier l'art. 13 Cst. de sorte qu'il soit mentionné que «toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications et de toutes les données qui lui sont propres» (al. 1) et que «ces données sont la propriété de la personne, qui doit être protégée contre leur emploi abusif» (al. 2). La Commission des institutions politiques du Conseil national a accepté de donner suite à l'initiative le 16 janvier 2015, celle du Conseil des Etats le 20 août 2015.

– Postulat Hodgers 10.3383 «Adapter la loi sur la protection des données aux nouvelles technologies». Cette intervention a été adoptée par le Conseil national le 1er octobre 2010. Elle demande au Conseil fédéral d'étudier la possibilité de renforcer la protection des données et le droit à la vie privée en modifiant la LPD pour l'adapter aux nouvelles technologies. Ce postulat a été partiellement réalisé par le rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données[24].

– Postulat Graber 10.3651 «Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles». Le Conseil national a adopté cette intervention le 17 décembre 2010. L'auteur demande au Conseil fédéral d'établir un rapport sur les risques que présentent les technologies de surveillance et la collecte de renseignements sur la sphère privée, sur les limites envisageables en définissant le cas échéant un noyau dur de la sphère privée inviolable et sur l'opportunité de renforcer la législation protectrice de la sphère privée et des données personnelles. Ce postulat a déjà été partiellement réalisé par le rapport du Conseil fédéral du 9 décembre 2011.

– Postulat Schwaab 12.3152 «Droit à l'oubli numérique». Cette intervention a été adoptée par le Conseil national le 15 juin 2012. Celle-ci charge le Conseil fédéral d'étudier l'opportunité de régler ou de préciser dans la législation un droit à «l'oubli numérique» et les modalités pour en faciliter l'usage par les consommateurs.

– Motion Rechsteiner 13.3841 «Commission d'experts pour l'avenir du traitement et de la sécurité des données». Cette motion demande la création d'une commission d'experts interdisciplinaire pour assurer au mieux à l'avenir le

23 RS **101**
24 FF **2012** 255, 270

traitement et la sécurité des données. Cette intervention a été adoptée par le Conseil des Etats le 3 décembre 2013 et par le Conseil national le 13 mars 2014. Les travaux y relatifs, rattachés au DFF, ont une portée qui dépasse le cadre du présent projet (cf. ch. 1.1.4). Ce dernier prévoit toutefois certaines mesures qui vont dans le sens de la réalisation de la motion.

– Postulat Recordon 13.3989 «Violations de la personnalité dues au progrès des techniques de l'information et de la communication». Le Conseil des Etats a adopté cette intervention le 11 décembre 2013. Celle-ci invite le Conseil fédéral à fournir un rapport sur les risques que les progrès des techniques de l'information et de la communication font courir aux droits de la personnalité et sur les solutions envisageables.

– Motion Comte 14.3288 «Faire de l'usurpation d'identité une infraction pénale en tant que telle»: cette intervention a été adoptée par les Chambres fédérales les 12 juin et 24 novembre 2014. Elle demande au Conseil fédéral de présenter une modification du droit pénal faisant de l'usurpation d'identité une infraction pénale en tant que telle.

– Postulat Derder 14.3655 «Définir notre identité numérique et identifier les solutions pour la protéger». Cette intervention a été adoptée par le Conseil national le 26 septembre 2014. L'auteur demande au Conseil fédéral un rapport permettant la définition de l'identité numérique des citoyens, l'intégrant dans leur personnalité juridique actuelle, couvrant l'empreinte des données personnelles potentiellement publiques, les menaces sur notre sphère privée et les manières de la protéger des activités d'entreprises ou de services de renseignements suisses ou étrangers.

– Postulat Schwaab 14.3739 «Control by design. Renforcer les droits de propriété pour empêcher les connexions indésirables»: le Conseil national a adopté cette intervention le 12 décembre 2014. L'auteur demande que le gouvernement évalue l'introduction dans la législation d'un «contrôle dès la conception» («control by design»), afin que le propriétaire ou possesseur d'une chose bénéficie du droit de s'opposer à la connexion de cette dernière à un quelconque réseau. Le Conseil fédéral est également invité à évaluer la pertinence d'adapter la législation par rapport au transfert de la propriété et de la possession ainsi qu'à la protection des données.

– Postulat Schwaab 14.3782 «Des règles pour la ‹mort numérique›». Le Conseil national a adopté cette intervention le 12 décembre 2014. Ce postulat charge le Conseil fédéral d'évaluer la pertinence de compléter le droit des successions afin de régler les droits des héritiers aux données personnelles et aux accès numériques du défunt ainsi que la conséquence de son décès sur sa présence virtuelle.

– Postulat Groupe libéral-radical 14.4137 «Enregistrements vidéo par des privés. Mieux protéger la sphère privée». Le postulat demande au Conseil fédéral d'établir un rapport qui mette l'accent sur les risques relatifs à l'utilisation des caméras privées dans des drones et des lunettes connectées. Il a été adopté par le Conseil national le 20 mars 2015.

– Postulat Comte 14.4284 «Enregistrements vidéo par des privés. Mieux protéger la sphère privée». Ce postulat a la même teneur que le postulat Groupe libéral-radical 14.4137 ci-dessus. Il a été adopté par le Conseil des Etats le 19 mars 2015.

– Postulat Derder 15.4045 «Droit d'exploiter des données personnelles. Droit d'obtenir une copie». Ce postulat demande au Conseil fédéral d'examiner dans quelle mesure les particuliers et l'économie pourraient profiter de la réutilisation de données à caractère personnel et disposer d'un droit d'obtenir une copie des données traitées à leur sujet. Le Conseil national a adopté cette intervention le 18 décembre 2015.

– Postulat Béglé 16.3383 «Données numériques, informer les personnes lésées en cas de piratage». Ce postulat demande au Conseil fédéral d'étudier l'opportunité d'obliger les organismes victimes d'un piratage informatique des données numériques sous leur responsabilité d'avertir les personnes lésées afin qu'elles puissent agir pour limiter les dommages. Ce postulat a été adopté par le Conseil national le 30 septembre 2016.

– Postulat Béglé 16.3384 «Données numériques médicales. Assurer une collecte protégée, transparente et ciblée dans la révision de la loi sur la protection des données». Il est demandé au Conseil fédéral d'étudier l'intégration dans la révision de plusieurs éléments afin d'offrir un maximum de garanties pour les données médicales: directives de sécurisation du stockage, de transmission et d'accès, élevées et homogènes pour tous les acteurs concernés; introduction d'un principe de «consentement véritable» du patient; principes de «*Privacy by default*» et de «*Privacy by design*»; sensibilisation des personnes concernées sur les dangers d'une transmission de certaines données personnelles. Ce postulat a été adopté par le Conseil national le 30 septembre 2016.

– Postulat Béglé 16.3386 «Réappropriation des données personnelles. Favoriser l'autodétermination informationnelle». Ce postulat charge le Conseil fédéral d'étudier le meilleur moyen de favoriser la réappropriation des données personnelles par les individus. Ce postulat a été adopté par le Conseil national le 30 septembre 2016.

– Postulat Schwaab 16.3682 «Encadrement des pratiques des sociétés de renseignements de solvabilité». Ce postulat demande au Conseil fédéral d'étudier la nécessité d'un meilleur encadrement des pratiques des sociétés de renseignements de solvabilité, notamment par le biais de l'introduction de limites claires en matière de méthodes utilisables pour obtenir des informations sur la solvabilité des particuliers et des entreprises. Conformément à la proposition du Conseil fédéral, le Conseil national a adopté le postulat le 16 décembre 2016.

– Initiative parlementaire 16.409 Leutenegger Oberholzer «Procédure de désignation du Préposé fédéral à la protection des données et à la transparence». Cette initiative demande que le préposé soit élu par l'Assemblée fédérale. La Commission des institutions politiques du Conseil national a décidé, le

20 janvier 2017, de donner suite à cette initiative. Celle du Conseil des Etats a décidé d'adhérer à cette décision le 31 mars 2017.

1.2 Contexte international

1.2.1 Remarques générales concernant la protection de la sphère privée au plan international

Navi Pillay, ancienne Haut-Commissaire des Nations Unies aux droits de l'homme, a présenté, le 16 juillet 2014, le rapport (A/HRC/27/37) «Le droit à la vie privée à l'ère du numérique» (voir ci-après ch. 1.2.4). Ce rapport donne une vue d'ensemble succincte des droits de l'homme par rapport à la protection de la sphère privée à l'ère numérique et tire un bilan mitigé de la situation juridique actuelle.

Au niveau international, il est de plus en plus reconnu que le traitement de données personnelles touche en principe la sphère privée et qu'il est susceptible d'affecter d'autres droits fondamentaux. Pour garantir une protection efficace de la sphère privée, des bases légales suffisantes doivent être créées pour justifier ces ingérences. Les droits que l'on peut invoquer hors ligne, doivent également être protégés en ligne. Outre le droit à la protection de la sphère privée, garanti par l'art. 13 Cst., mais aussi par plusieurs conventions internationales contraignantes (Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel [convention STE 108][25]; art. 8 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales [CEDH][26], art. 17 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques [Pacte ONU II][27]), d'autres droits peuvent être touchés: les libertés d'opinion et d'information (art. 16 Cst., art. 10 CEDH, art. 19 Pacte ONU II), la liberté de réunion (art. 22 Cst., art. 11 CEDH, art. 21 Pacte ONU II), ou la liberté d'association (art. 23 et 28 Cst., art. 11 CEDH, art. 22 Pacte ONU II).

La limitation de la protection de la sphère privée doit en particulier respecter les exigences fixées à l'art. 8, par. 2, CEDH (nécessité d'une base légale, existence d'un motif justificatif, proportionnalité). La Cour européenne des droits de l'homme (CEDH) laisse en principe aux parties une large marge d'appréciation en ce qui concerne la légitimité du but poursuivi[28]. Elle est en revanche très exigeante en ce qui concerne l'exigence de la base légale: la norme autorisant l'atteinte doit être suffisamment claire et prévoir des mesures contre une utilisation abusive des données, ainsi qu'un droit d'accès pour la personne. La loi doit par ailleurs préciser qui peut traiter quelles données, à quelles fins, combien de temps ces données peuvent être conservées et la manière de vérifier le respect de ces conditions. Des exigences plus strictes sont prévues pour les données sensibles.

25 RS **0.235.1**
26 CEDH, RS **0.101**
27 Pacte ONU-II, RS **0.103.2**
28 Voir par exemple CEDH 59842/00 (Vetter c. France) du 31.8.2005; CEDH 44647/98 (Peck c. UK) du 28.1.2003; CEDH 27798/95 (Amann c. Switzerland) du 16.2.2000.

1.2.2 Union européenne

1.2.2.1 Réglementation pertinente

L'Union européenne a adopté, ces dernières décennies, plusieurs textes législatifs en vue de protéger les données à caractère personnel. Le texte principal est la directive 95/46/CE du 24 octobre 1995[29] relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après «directive 95/46/CE»). Celle-ci a été complétée par la décision-cadre 2008/977/JAI[30] du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (ci-après «décision-cadre 2008/977/JAI»).

Dans le cadre du programme de Stockholm[31], l'Union européenne a exprimé sa volonté de disposer d'une nouvelle législation uniforme en matière de protection des données, afin notamment de garantir le droit fondamental des personnes à la protection de leurs données personnelles, de permettre le développement de l'économie numérique et d'améliorer la lutte contre la criminalité et le terrorisme. Le Conseil européen a dès lors invité la Commission européenne à évaluer le fonctionnement de la directive 95/46/CE et de la décision-cadre 2008/977/JAI et à lui présenter le cas échéant de nouvelles initiatives en matière de protection des données. Dans sa communication du 4 novembre 2010 intitulée «une approche globale de la protection des données à caractère personnel dans l'Union européenne»[32], la Commission européenne a conclu que l'Union européenne avait besoin d'une politique plus globale et plus cohérente à l'égard du droit fondamental à la protection des données à caractère personnel.

Le 27 avril 2016, le Parlement européen et le Conseil de l'Union européenne ont adopté une réforme de la législation sur la protection des données qui comprend deux actes législatifs. Il s'agit d'une part du règlement (UE) 2016/679, qui remplacera la directive 95/46/CE (voir ci-après ch. 4). Le second acte adopté est la directive (UE) 2016/680, qui remplacera la décision-cadre 2008/977/JAI (voir ci-après ch. 2).

La directive (UE) 2016/680 constitue pour la Suisse un développement de l'acquis de Schengen; celle-ci doit donc le reprendre en vertu de l'accord d'association à Schengen. En revanche, la Suisse n'est pas tenue de reprendre le règlement (UE) 2016/679 car, selon l'Union européenne, il ne constitue pas un développement de l'acquis de Schengen.

Dans le cadre de sa Stratégie pour un marché unique numérique en Europe, la Commission européenne a présenté, le 10 janvier 2017, une proposition pour un «Règlement sur la vie privée et les communications électroniques». Ce texte est amené à remplacer la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée

29 JO L 281 du 23.11.1995, p. 31.
30 JO L 350 du 30.12.2008, p. 60.
31 JO C 115 du 4.5.2010, p. 1.
32 COM (2010) 609 final.

et communications électroniques)[33]. Ce règlement sera une *lex specialis* par rapport au règlement (UE) 2016/679. Il le précise et le complète s'agissant des communications électroniques[34]. Il ne constitue pas un développement des acquis de Schengen.

1.2.2.2 Décision d'adéquation

Dans les domaines qui ne relèvent pas de la coopération instaurée par Schengen et Dublin, la Suisse est considérée comme un Etat tiers. Or, l'échange de données entre un Etat tiers et les Etats membres de l'Union européenne ne peut se faire que si le pays tiers assure un niveau de protection adéquat au sens de la directive 95/46/CE. Ce niveau de protection fait régulièrement l'objet d'une évaluation de la Commission européenne, qui rend, le cas échéant, une décision d'adéquation. Cette dernière peut être révoquée en tout temps.

Par décision du 26 juillet 2000, la Commission européenne a constaté que la Suisse dispose d'un niveau de protection adéquat des données[35]. Cette décision se fonde toutefois sur le niveau de protection défini par la directive 95/46/CE.

Par courrier du 25 janvier 2017, la Commission européenne a informé la Mission de la Suisse auprès de l'Union européenne que, suite à un arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 (affaire «Schrems»), elle est tenue de procéder à un suivi périodique du niveau de protection adéquat des données assuré par les Etats tiers qui sont au bénéfice d'une décision d'adéquation. La Commission européenne a dès lors demandé à la Suisse de lui faire parvenir un rapport présentant la situation légale en matière de protection des données et les principales modifications législatives intervenues depuis 2000. Ce rapport sera transmis à la Commission européenne d'ici fin 2017.

A l'avenir, l'examen de la législation suisse se fera à la lumière des exigences contenues dans le règlement (UE) 2016/679. Si la Suisse souhaite conserver la décision d'adéquation dont elle bénéficie ou si, en cas de révocation, elle entend obtenir à nouveau une telle décision – ce qui est très important pour l'économie – il est essentiel que sa législation offre une protection équivalente aux exigences du règlement (UE) 2016/679.

1.2.2.3 Recommandations suite à l'évaluation Schengen

En s'associant à Schengen-Dublin, la Suisse s'est engagée à ce que les traitements de données personnelles effectués dans le cadre de la coopération Schengen soient conformes à la réglementation de l'Union européenne applicable en matière de protection des données, en particulier la directive 95/46/CE et la décision-cadre 2008/977/JAI.

33 JO L 201, 31.7.2002, pp. 37-47.
34 Proposition, ch. 1.2 de l'*Explanatory memorandum*.
35 Décision de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse, JO L 215 du 25.8.2000, p. 1.

Dans le cadre du mécanisme d'évaluation Schengen, l'Union européenne évalue périodiquement les Etats Schengen, dont la Suisse, afin de contrôler si ceux-ci respectent leurs engagements. La dernière évaluation Schengen de la Suisse a eu lieu durant le premier semestre 2014.

Le 11 septembre 2014, le Conseil de l'Union européenne a adopté le rapport du comité d'évaluation concernant la protection des données en Suisse dans le domaine de la coopération Schengen. Selon les conclusions de ce rapport, la législation suisse en matière de protection des données est conforme aux exigences de l'acquis de Schengen. Le rapport d'évaluation contient toutefois une recommandation qui invite la Suisse à renforcer les pouvoirs du préposé en lui attribuant des pouvoirs décisionnels. Le comité d'évaluation note au surplus que le renforcement de ses pouvoirs de sanction serait bienvenu. La Suisse aura à rendre compte de la manière dont elle a mis en œuvre les recommandations des experts lors de la prochaine évaluation qui aura lieu en 2018.

Le P-LPD donne suite aux recommandations du Conseil de l'Union européenne, dans la mesure où des compétences décisionnelles sont conférées au préposé (cf. art. 45 et 46 P-LPD). Par contre, le Conseil fédéral est arrivé à la conclusion qu'il n'est pas opportun de conférer au préposé la compétence de prononcer des sanctions administratives à l'encontre des organes fédéraux, au motif qu'une telle possibilité, qui existe dans d'autres pays, n'est pas conforme à notre tradition juridique. Le Conseil fédéral considère que la possibilité pour le préposé d'interdire ou de suspendre un traitement effectué par un organe fédéral, ainsi que le renforcement du volet pénal de la loi, constituent des mesures suffisantes.

1.2.3 Conseil de l'Europe (convention STE 108)

Le Conseil de l'Europe a adopté, le 28 janvier 1981, le premier traité international en matière de protection des données, à savoir la convention STE 108, qui a été ratifiée par la Suisse le 2 octobre 1997. Cette convention a été complétée par le protocole additionnel du 8 novembre 2001 à la convention STE 108 concernant les autorités de contrôle et les flux transfrontières de données[36] (STE 181, ci-après «protocole additionnel») que la Suisse a également ratifié, le 20 décembre 2007. La convention a entretemps été ratifiée par d'autres Etats qui ne sont pas membres du Conseil de l'Europe (cf. ch. 3.1).

En 2011, le Conseil de l'Europe a entamé une procédure de modernisation de la convention STE 108 et de son protocole additionnel, avec pour objectif de mieux répondre aux défis que représentent la globalisation, les évolutions technologiques et l'augmentation des flux transfrontières des données pour la protection de la sphère privée et des droits fondamentaux des personnes concernées. Sous présidence suisse, le Comité consultatif de la convention STE 108 a élaboré un projet de modernisation de la convention. Les travaux du Comité ad hoc établi par le Comité des Ministres (CAHDATA) se sont terminés en juin 2016. Le protocole d'amendement de la convention STE 108 doit encore être adopté par le Comité des Ministres (voir ci-après

36 RS **0.235.11**

ch. 3.2). Le présent message se base sur le projet de modernisation dans sa version de septembre 2016[37], qui ne devrait plus subir de modifications substantielles.

Le P-STE 108 a un contenu très semblable à celui de la directive (UE) 2016/680 et du règlement (UE) 2016/679. Il est toutefois moins détaillé et moins dense. La Commission européenne, qui représentait les Etats membres de l'Union européenne lors des négociations, a veillé à ce que le texte du P-STE 108 soit compatible avec le nouveau droit de l'Union européenne.

1.2.4 Nations Unies

Le droit à la sphère privée est devenu, depuis l'affaire Snowden, un thème prioritaire pour plusieurs institutions onusiennes. Ainsi, en décembre 2013, l'Assemblée générale a adopté une résolution[38] qui appelle chaque Etat à revoir sa législation afin de protéger le droit à la vie privée. Par ailleurs, elle demande au Haut-commissariat des Nations unies aux droits de l'homme (HCDH) de rédiger un rapport sur «la protection et la promotion du droit à la vie privée dans le contexte de la surveillance et de l'interception des communications numériques et de la collecte des données personnelles sur le territoire national et à l'extérieur, y compris à grande échelle». Ce rapport a été présenté en juillet 2014[39]. Par ailleurs, le Conseil des droits de l'homme a créé en mars 2015 un poste de rapporteur spécial sur le droit à la vie privée, pour une durée de trois ans. Ce dernier est chargé d'analyser les défis en matière de protection de la vie privée, dans le contexte notamment de la fulgurante évolution technologique et des nouvelles possibilités de surveillance de la communication privée qui en découlent. La Suisse a soutenu ces deux initiatives et y a participé activement.

Le rapporteur spécial a rendu deux rapports à ce jour, l'un le 8 mars 2016[40] et l'autre le 27 février 2017[41].

Dans son premier rapport, il dresse un aperçu de la situation en matière de protection de la vie privée début 2016 et présente un plan d'action pour les trois premières années de son mandat. Il relève notamment que l'absence de définition universelle contraignante de la notion de sphère privée constitue l'un des principaux obstacles à une protection juridique complète de celle-ci. Il constate aussi que, globalement, les craintes quant à une utilisation abusive des données, auparavant dirigée contre l'Etat, se sont reportées sur les entreprises et qu'il est nécessaire d'établir un dialogue au niveau international sur la manière dont les entreprises collectent et traitent les données personnelles et les transmettent à des services étatiques[42]. Il observe en outre une prise de conscience des consommateurs sur les risques qui pèsent sur leur sphère privée, comme en témoigne par exemple le développement rapide d'un marché des

37 Le texte français peut être consulté à l'adresse suivante: rm.coe.int/16806b6f7b.
38 Résolution 68/167 du 18 décembre 2013 disponible en français sous le lien suivant: www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167.
39 HCDH «Le droit à la vie privée à l'ère du numérique», 2014.
40 A/HRC/31/64
41 A/HRC/34/60
42 A/HRC/31/64, ch. 9 et ch. 46 s.

produits et services respectueux de la sphère privée[43]. Enfin, il reconnaît l'importance de l'industrie des produits dotés d'une protection biométrique, en plein développement, et exprime son intention de travailler de concert avec les chercheurs, les autorités de poursuite pénale, les services de renseignements ainsi que la société civile pour trouver des mécanismes de protection adaptés, aussi bien sur le plan technique que sur le plan légal[44].

Le second rapport met l'accent sur les mesures de surveillance étatique aux plans national et international. Il décrit les derniers développements et tendances, et esquisse quelques pistes pour assurer un contrôle de cette surveillance. Il propose en particulier d'élaborer un instrument international pour la protection de la sphère privé dans le cyberespace. Le rapporteur spécial voit ses revendications comme un complément aux instruments en vigueur (comme par ex. la Convention du Conseil de l'Europe sur la cybercriminalité, du 13 novembre 2001[45]) et aux différentes initiatives au niveau international[46].

La Suisse suit ces développements avec attention.

1.2.5 Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

Les lignes directrices de l'Organisation de coopération et de développement économiques (OCDE) régissant la protection de la vie privée[47] – élaborées en 1980 et révisées en 2013 – ont principalement pour but, conformément à l'orientation économique de cette organisation, l'harmonisation des niveaux de protection des données nationaux. Les lignes directrices doivent, tout en préservant les droits fondamentaux, permettre d'instaurer une réglementation assurant l'échange de données et d'informations au plan international et évitant les entraves au commerce. Bien que les lignes directrices ne soient que des recommandations et qu'elles n'aient pas d'effets juridiques contraignants, elles ont eu une forte influence sur le développement de la réglementation en matière de protection des données aux niveaux national et international.

Le champ d'application des lignes directrices s'étend à l'ensemble des données du secteur public et privé qui, en raison de leur nature, de leur mode de traitement ou du contexte dans lequel elles sont utilisées, présentent un risque pour la sphère privée et les autres libertés individuelles. Elles arrêtent huit principes fondamentaux, conçus comme des standards minimaux, qui visent à trouver un équilibre entre la protection

43 A/HRC/31/64, ch. 50.
44 A/HRC/31/64, ch. 15 et 46*e*.
45 RS **0.311.43,** ratifiée par la Suisse le 21 septembre 2011.
46 Voir par exemple le «MAPPING-project»; www.mappingtheinternet.eu/.
47 Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980, consultables à l'adresse: www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm; OECD Guidelines governing the protection of privacy and transborder flows of personal data, 2013, consultables à l'adresse: www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

de la sphère privée et le libre flux d'informations (principes de la limitation de la collecte, de la qualité des données, de la finalité, de la limitation de l'utilisation, des garanties de sécurité, de la bonne foi, de la participation individuelle et de la responsabilité)[48]. Les lignes directrices révisées sont entrées en vigueur en juillet 2013; elles contiennent plusieurs précisions et compléments. A titre d'exemple, les critères régissant le transfert de données à l'étranger ont été précisés, et la coopération internationale a été renforcée[49]. Les lignes directrices révisées prévoient explicitement que les responsables du traitement assument la responsabilité de toutes les données personnelles placées sous leur contrôle, indépendamment de l'endroit où elles se trouvent[50]. Enfin, il est prévu que les échanges de données avec des pays non-membres de l'OCDE ne peuvent pas être limités si ces derniers se conforment aux lignes directrices de protection des données ou s'il existe des garanties que le niveau de protection exigé par ces lignes directrices est respecté.

1.3 Objectifs du projet

Le projet donne suite au mandat conféré par le Conseil fédéral au DFJP de préparer un avant-projet de loi, en tenant compte des conclusions du rapport du 29 octobre 2014 intitulé «esquisse d'acte normatif relative à la révision de la loi sur la protection des données» ainsi que des réformes du Conseil de l'Europe et de l'Union européenne. L'adoption du message figure également parmi les objectifs du Conseil fédéral de 2017 et dans le programme de la législature 2015 à 2019 (ch. 12.1). Le message réalise également une grande partie des interventions parlementaires figurant sous ch. 1.1.5.

Le projet de loi poursuit plusieurs objectifs qui se complètent mutuellement.

Il vise premièrement à adapter la législation suisse aux évolutions technologiques, qui ont des conséquences importantes sur la protection des données. Dans ce cadre, il s'agit tout d'abord, notamment, de rendre aux personnes concernées le contrôle de leurs données. Ces dernières, avec l'évolution de la société digitale, font en effet l'objet de collectes massives («Big Data») et de traitements qui sont de moins en moins transparents (par ex. profilage basé sur des algorithmes). Il s'agit ensuite de responsabiliser les responsables du traitement. Ils doivent en particulier prendre en considération les enjeux de protection des données dès la conception de nouveaux traitements et mettre en place, par défaut, la solution la plus favorable à la protection des données. Enfin, il s'agit de maintenir et de renforcer la compétitivité de la Suisse en créant un environnement propre à faciliter les flux transfrontières de données et à améliorer son attractivité pour de nouvelles activités en lien avec la société numérique, ce qui passe par un standard de protection élevé, reconnu au plan international.

48 OCDE, Lignes directrices régissant la protection de la vie privée 1980, principes 6 à 14; OECD, Privacy Framework 2013, pp. 22 et 47 s.
49 OECD, Lignes directrices régissant la protection de la vie privée 2013, principes 16 à 18, 19 let. g et 20 à 23.
50 OCDE, Lignes directrices sur la protection de la sphère privée, principe 16.

Le projet a ensuite pour objectif d'intégrer dans la législation suisse certains développements du droit de l'Union européenne. Ces derniers ont, dans le domaine de la protection des données, une grande importance, dans la mesure où les flux transfrontières de données personnelles font partie du quotidien. Il s'agit tout d'abord de la directive (UE) 2016/680, qui est un développement de l'acquis de Schengen que la Suisse s'est engagée à reprendre. Le projet doit ensuite mettre en œuvre les recommandations émises par l'Union européenne en 2014 à la suite de l'évaluation de la Suisse dans le cadre de l'accord d'association à Schengen. Les experts européens ont en effet notamment recommandé à la Suisse de doter le préposé de compétences décisionnelles (ch. 1.2.2.3). Enfin, le projet doit permettre de rapprocher la législation suisse du règlement (UE) 2016/679. Ce rapprochement est en effet nécessaire pour que la Suisse puisse continuer de bénéficier de la décision de la Commission européenne reconnaissant qu'elle offre un niveau de protection des données adéquat (ch. 1.2.2.2).

Pour terminer, le projet doit permettre à la Suisse de rendre sa législation compatible avec le P-STE 108. Il est en effet dans son intérêt de pouvoir ratifier la convention modernisée le plus vite possible, eu égard notamment à la décision d'adéquation de la Commission européenne. La ratification de la convention révisée sera en effet un élément important dans l'examen du maintien ou non de cette décision. Vu que le texte du P-STE est en principe définitif et que son contenu correspond en grande partie (mais en moins détaillé) à celui de la directive (UE) 2016/680 et du règlement (UE) 2016/679, le Conseil fédéral a décidé d'anticiper et d'intégrer les explications y relatives dans le présent message.

En résumé, le projet permet d'une part d'adapter la législation suisse aux nouvelles technologies. D'autre part, il permet de s'assurer que la Suisse remplit ses obligations découlant de l'accord d'association à Schengen, qu'elle pourra ratifier la convention STE 108 révisée et qu'elle continuera à figurer dans la liste des Etat tiers bénéficiant d'une décision d'adéquation de la Commission européenne, décision qui profite en particulier aux milieux économiques.

Le présent projet implique ainsi une révision totale de la LPD (qui inclut aussi la révision de certaines lois spéciales), et une révision partielle des lois spéciales applicables au domaine de la coopération policière et judiciaire instaurée par Schengen.

1.4 Présentation du P-LPD

1.4.1 Grandes lignes de la révision

Le projet repose sur sept principes de base, autour desquels les différentes nouveautés s'articulent.

Selon un premier principe, la révision se base sur une *approche fondée sur le risque*, plus précisément sur les risques potentiels encourus par les personnes concernées. En effet, les menaces qui pèsent sur leur sphère privée dépendent dans une large mesure des activités menées par les responsables du traitement et par les sous-traitants. Pour cette raison, les obligations sont plus strictes pour les responsables du traitement dont les activités présentent des risques accrus (par ex. entreprises dont

l'essentiel des activités réside dans le traitement de données) que pour ceux dont les activités sont moins risquées (par ex. traitements des données d'un fichier de clients ne contenant pas de données sensibles).

Un second principe réside dans la *neutralité technologique* du projet. A l'instar de la loi en vigueur, le P-LPD traite dans la mesure du possible de manière égale les différentes technologies. La loi peut ainsi s'adapter aux évolutions technologiques sans freiner l'innovation.

Selon un troisième principe, la *terminologie* de la loi est *modernisée*. Cela a notamment pour objectif d'améliorer la compatibilité du droit suisse avec le droit de l'Union européenne. Pour cette raison, certaines définitions contenues dans les textes européens sont reprises. La notion de «maître du fichier» est ainsi remplacée par celle de «responsable du traitement». La notion de «profil de la personnalité» qui constitue une particularité suisse, disparaît au profit de la notion de «profilage». La notion de «données sensibles» est étendue aux «données génétiques» et aux «données biométriques».

Un quatrième principe est l'*amélioration des échanges de données transfrontières*. La réglementation régissant la communication de données à l'étranger est complétée sur certains points. Le principe selon lequel aucune donnée personnelle ne peut être communiquée à l'étranger en l'absence d'un niveau de protection adéquat est supprimé en raison de l'insécurité juridique qui en découle. Des données pourront être transmises à l'étranger si Conseil fédéral a constaté, par voie d'ordonnance, que le pays destinataire ou l'organisme international offre un niveau de protection adéquat des données. A défaut d'une telle décision, le P-LPD prévoit divers moyens de garantir une protection suffisante des données, de sorte que leur communication à l'étranger reste possible.

Un cinquième principe de la révision, particulièrement important, est le *renforcement des droits de la personne concernée*. Différents instruments sont prévus pour qu'elle ait un meilleur contrôle sur ses données et qu'elle puisse mieux décider de leur utilisation. Les conditions déterminant le consentement valable de la personne concernée sont notamment précisées.

Le sixième principe est étroitement lié au cinquième. Il vise à préciser les *obligations des responsables du traitement*, en les orientant plus sur la protection de la personne concernée. Le P-LPD définit ainsi plus en détail l'obligation d'informer et impose aux responsables du traitement de procéder dans certains cas à une analyse d'impact relative à la protection des données. Des mesures techniques doivent par ailleurs assurer un paramétrage des systèmes qui garantit au mieux la protection des données. Ces nouvelles obligations sont compensées par certains allégements. Ainsi, il est proposé de supprimer l'obligation pour le secteur privé de déclarer les fichiers de traitement des données au préposé.

Le septième principe vise le *renforcement des contrôles*. Il est prévu de renforcer le rôle et l'indépendance du préposé. Ses pouvoirs sont comparables à ceux des autorités de contrôle des autres pays. A la différence de la plupart de ses homologues européens, il n'est toutefois pas habilité à prononcer des sanctions administratives. En compensation, les dispositions pénales de la loi sont renforcées.

1.4.2 Principales nouveautés

1.4.2.1 Modification du champ d'application de la future LPD

Le P-LPD propose de renoncer à la protection des données des personnes morales; les textes de protection des données de l'Union européenne et du Conseil de l'Europe, ainsi que ceux de la majorité des pays étrangers, ne prévoient pas une telle protection. Cette dernière a peu de portée pratique et sa suppression ne devrait pas avoir de conséquences négatives, vu notamment la protection conférée par d'autres lois dans des secteurs particuliers (protection de la personnalité, concurrence déloyale, droit d'auteur). Cette modification devrait faciliter la communication de données vers des Etats étrangers dont la législation ne connaît pas la protection des données des personnes morales.

En ce qui concerne le secteur public, l'abrogation de la protection des données des personnes morales a pour conséquence que les bases légales prévues par le droit fédéral qui habilitent les organes fédéraux à traiter des données personnelles ne s'appliquent plus lorsque ceux-ci traitent des données concernant des personnes morales. Or l'art. 5 Cst. exige que l'activité de l'Etat soit régie par la loi. De plus, les personnes morales bénéficient de la protection de la sphère privée, bien qu'elles ne soient pas titulaires de tous les aspects protégés par l'art. 13 Cst.[51]. Le Conseil fédéral propose par conséquent de créer une série de dispositions légales dans la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[52], qui règlent la marche à suivre concernant les traitements de données concernant des personnes morales par les organes fédéraux (cf. ch. 9.2.8). Par ailleurs, une disposition transitoire permet d'éviter l'apparition de lacunes juridiques pendant cinq ans (art. 66 P-LPD et les explications sous ch. 9.1.11).

1.4.2.2 Renforcement de la transparence des traitements de données et de la maîtrise de leurs données par les personnes concernées

La transparence des traitements est améliorée: le devoir d'information lors de la collecte est étendu à tous les traitements dans le secteur privé. Il est assorti d'exceptions et peut être rempli de manière standardisée. Le projet introduit un devoir d'information lors de décisions individuelles automatisées, ainsi que le droit pour la personne concernée, à certaines conditions, de faire valoir son point de vue et d'exiger qu'une personne physique revoie la décision. Le projet de loi étend également la liste des informations à fournir à la personne concernée lorsque celle-ci exerce son droit d'accès.

51 ATF **137** II 371, consid. 6.
52 RS **172.010**

Les droits des personnes concernées sont clarifiés sur différents points. Entre autres, le P-LPD mentionne expressément le droit à l'effacement des données, ce que la LPD ne fait que de manière implicite. De plus, l'accès à la justice est facilité par la suppression des frais judiciaires en procédure civile.

Pour tenir compte des résultats de la consultation externe, les différents devoirs des responsables du traitement et les droits des personnes concernées ont été retravaillés de manière à ne pas poser des exigences plus strictes que le droit européen.

1.4.2.3 Encouragement de l'autoréglementation

La révision encourage le développement de l'autoréglementation et la responsabilisation des responsables du traitement. Vu les résultats de la consultation externe, le mécanisme a été retravaillé. Il est désormais prévu que les associations professionnelles et les associations économiques qui élaborent des codes de conduite puissent les soumettre au préposé. Ce dernier doit prendre position et publier sa prise de position.

Les codes de conduite élaborés par les branches permettent de préciser certaines notions, les modalités de certains droits ou de certains devoirs.

Ces codes ne sont pas obligatoires.

1.4.2.4 Renforcement du statut, des pouvoirs et des tâches du préposé

Le statut et l'indépendance du préposé sont renforcés. Ce dernier peut effectuer trois mandats au maximum et ne peut exercer une activité accessoire qu'à des conditions strictes. Le P-LPD prévoit en outre que le préposé peut, à l'instar de ses homologues européens, prendre des décisions contraignantes à l'égard des responsables du traitement et des sous-traitants, au terme d'une enquête ouverte d'office ou sur dénonciation. Seuls l'organe fédéral et la personne privée contre qui l'enquête a été ouverte ont qualité de partie à la procédure.

1.4.2.5 Renforcement des sanctions pénales

Le volet pénal de la LPD est renforcé à plusieurs égards, pour compenser notamment le fait que le préposé, contrairement à ses homologues européens, n'a pas le pouvoir d'infliger des sanctions administratives. Ce renforcement comprend notamment: l'augmentation du seuil maximum des amendes à 250 000 francs; l'adaptation de la liste des comportements punissables aux nouvelles obligations des responsables du traitement; l'institution d'une contravention pour insoumission à une décision du préposé ou d'une autorité de recours; l'octroi de la possibilité, pour le préposé, de faire valoir les droits d'une partie plaignante dans le cadre d'une procédure pénale, ou encore la prolongation du délai de prescription de l'action pénale. En cas d'infraction commise dans une entreprise, les autorités de poursuite pénale

peuvent, à certaines conditions, renoncer à rechercher les personnes responsables et condamner directement l'entreprise au paiement de l'amende.

Le code pénal (CP)[53] est par ailleurs complété par un art. 179decies, une disposition punissant l'usurpation d'identité d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.

Le système des sanctions pénales, déjà prévu dans l'avant-projet (art. 50 ss), a été la cible de nombreuses remarques. La principale critique provient du fait que les sanctions pénales visent les personnes physiques au premier chef, alors que, selon les participants, les entreprises devraient être exclusivement punissables, par le biais de sanctions administratives prononcées par le préposé (ou par une commission créée à cet effet). On craint que de simples employés, sans pouvoir de décision, ne soient condamnés. La sévérité des sanctions, en particulier le montant des amendes, le manque de précision de certains états de fait et le catalogue des comportements punissables, de même que le fait de punir la négligence, ont également fait l'objet de nombreuses critiques.

Le projet tient compte de ces critiques en réduisant, par rapport à l'avant-projet, le catalogue des comportements punissables et le montant des amendes, et en supprimant la négligence.

Pour ce qui est de la punissabilité directe des entreprises par le biais de sanctions administratives, le Conseil fédéral y renonce. Il est d'avis que l'introduction de telles sanctions dans la LPD n'est pas souhaitable. Ces sanctions, qui présentent un caractère pénal, doivent en effet rester exceptionnelles et se limiter à des secteurs dans lesquels le cercle des destinataires est limité (notamment cartels, jeux d'argent). A défaut de règles de procédure applicables spécifiquement à de telles sanctions, on court le risque de voir les garanties de procédure dont devraient bénéficier les contrevenants, violées.

La crainte que n'importe quel employé d'une entreprise traitant des données puisse être condamné est infondée. La plupart des comportements punissables concernent en effet le responsable du traitement. Lorsque ce dernier est une entreprise, l'infraction est alors imputée aux représentants des organes dirigeants, en application de l'art. 29 CP. Il en va notamment ainsi en cas d'insoumission à une décision du préposé: est alors punissable la personne responsable qui, au sein de l'entreprise, aurait dû faire exécuter la décision administrative du préposé. Le projet renforce en outre la responsabilité des organes dirigeants en rendant applicable l'art. 6 de loi fédérale du 22 mars 1974 sur le droit pénal administratif (DPA)[54] (imputabilité des infractions commises au sein d'une entreprise). Enfin, il permet de sanctionner directement l'entreprise lorsque le montant de l'amende prévisible ne dépasse pas 50 000 francs et que l'identification de la personne punissable nécessite des actes d'enquête disproportionnés.

53 RS **311.0**
54 RS **313.0**

1.5 Présentation de la révision d'autres lois fédérales

Dans les lois spéciales applicables aux domaines de coopération policière et judiciaire instaurée par Schengen, le projet de loi introduit une obligation pour l'autorité compétente d'établir, dans la mesure du possible, une distinction entre les différentes catégories de personnes concernées ainsi qu'entre les données fondées sur des faits et celles découlant d'appréciations personnelles. Les droits des personnes concernées sont également renforcés. Ainsi, celles-ci peuvent, à certaines conditions, exiger du préposé qu'il vérifie la licéité des traitements de données les concernant. En cas de traitements illicites de leurs données, elles peuvent de plus requérir du préposé l'ouverture d'une enquête qui peut, le cas échéant, aboutir à une décision susceptible de recours. Enfin, le projet de loi règle les conditions de protection des données applicables aux communications de données effectuées entre Etats Schengen ou entre une autorité suisse et un Etat tiers dans le cadre de la coopération judiciaire et policière instaurée par Schengen.

1.6 Appréciation de la solution retenue

1.6.1 Evaluation des résultats de la consultation externe

Au total, 222 prises de position ont été reçues[55]. Sur les participants qui ont été officiellement invités, ont pris position trois tribunaux fédéraux, tous les cantons, sept partis politiques, l'Union des villes suisses ainsi que onze organisations. En outre, 178 participants issus des milieux concernés se sont également exprimés sur le sujet.

Sur le principe, aucun des participants ne s'oppose à une nouvelle réglementation en matière de protection des données. Une majorité des participants l'approuve même expressément. La reprise de la directive (UE) 2016/680 et des exigences du P-STE 108 n'est pas contestée.

Pratiquement tous les participants ont formulé des remarques. Ces dernières portent presque exclusivement sur l'AP-LPD. On peut relever deux grandes tendances. Pour une majorité, l'avant-projet crée des charges administratives trop élevées et va sur certains points inutilement au-delà des exigences européennes, s'agissant des obligations des responsables du traitement principalement. Pour d'autres, le projet ne va au contraire pas suffisamment loin et devrait contenir des mesures supplémentaires pour renforcer la protection des personnes concernées.

Les principales remarques sont les suivantes:

– Terminologie: l'AP-LPD prévoyait une modernisation de la terminologie légale en reprenant certaines notions européennes. La suppression de la notion de «profil de la personnalité» et l'introduction de celle de «profilage»sont en particulier bien vues par une majorité des participants. La plu-

55 Le rapport sur la consultation externe est disponible sur le site Internet de l'OFJ: www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

part estiment cependant que cette dernière définition est trop large (art. 3, let. f, de l'AP-LPD) et qu'il faudrait se calquer sur celle du droit européen.

– Obligations des responsables du traitement et droits des personnes concernées: les différentes obligations des responsables du traitement, en particulier certains devoirs d'annonce auprès du préposé, sont jugées trop bureaucratiques par un grand nombre de participants issus de l'économie. Les petites et moyennes entreprises en particulier seraient, selon eux, bien en peine de respecter leurs obligations en la matière, faute de service juridique adéquat et de moyens. Cela concerne principalement les communications à l'étranger (art. 5 et 6 AP-LPD), les devoirs d'information (art. 13, 14 et 16 AP-LPD) et l'analyse d'impact relative à la protection des données (art. 16 AP-LPD). Sur certains points, l'AP-LPD irait par ailleurs sans raisons au-delà des exigences du droit européen.

– Autorégulation: la volonté du Conseil fédéral d'encourager l'autorégulation est saluée. Cependant, le système des recommandations de bonnes pratiques tel que prévu par les art. 8 et 9 AP-LPD ne convainc pas. Les milieux économiques s'opposent très largement à ce que le préposé ait lui-même l'initiative d'édicter de telles recommandations. Ils estiment que cette faculté doit appartenir aux branches exclusivement, qui sont plus à même de juger des spécificités de leur secteur. Le préposé aurait par ailleurs un statut de quasi législateur, sans pour autant jouir d'une quelconque légitimité démocratique, car ses recommandations seraient dans les faits suivies par les autorités. L'approbation des recommandations des branches par le préposé est aussi critiquée, en raison notamment de l'absence de voies de recours. Pour certains participants, l'instrument des recommandations de bonnes pratiques, faute d'être obligatoire, ne servira à rien. D'autres enfin estiment que le préposé n'aura en pratique pas les ressources suffisante pour élaborer des recommandations efficaces, si bien que les art. 8 et 9 AP-LPD resteront lettre morte.

  Un certain nombre de participants regrettent que l'AP-LPD ne mentionne plus la faculté de nommer des conseillers à la protection des données. Les milieux économiques souhaitent à cet égard que les responsables du traitement qui en ont institué puissent bénéficier de certains allégements administratifs.

– Statut et nomination du préposé: Certains participants contestent le processus de sa nomination et demandent qu'il soit élu directement et exclusivement par le Parlement. Par ailleurs, certains cantons souhaitent une indépendance budgétaire du préposé. La limitation du nombre de mandats du préposé ainsi que l'interdiction qui est faite au préposé d'exercer une activité accessoire dans un canton ou dans une commune sont aussi contestées, principalement par certains cantons. Enfin, de nombreux participants issus des milieux économiques s'opposent à la réélection tacite du préposé, pourtant déjà prévue par le droit actuel.

– Régime des sanctions: les dispositions pénales prévues par l'AP-LPD (art. 50 ss) ont été la cible de nombreuses critiques durant la procédure de consultation. Beaucoup de participants désirent une refonte totale du système prévu. La principale critique provient du fait que les sanctions pénales visent les personnes physiques au premier chef, alors que, selon les participants, elles devraient être d'ordre administratif et pouvoir être directement infligées à l'encontre des entreprises par le préposé (ou par une commission créée à cet effet). On craint que de simples employés, sans pouvoir de décision, ne soient condamnés.

  Les cantons sont également majoritairement opposés au maintien de la compétence cantonale de poursuivre et juger les infractions. Ils estiment que le nombre plus important de comportements incriminés et la sévérité accrue des sanctions vont provoquer une augmentation du nombre de procédures et nécessiter l'engagement de collaborateurs spécialisés.

  La sévérité des sanctions, en particulier le montant des amendes, le manque de précision de certains états de fait et le catalogue des comportements punissables ont également fait l'objet de nombreuses critiques.

  Divers participants issus des milieux économiques proposent une variante. En substance, elle repose sur un système de sanctions administratives pour les entreprises, prononcées par une «commission de protection des données» qui pourrait être rattachée au DFI ou au DFJP. Le catalogue des sanctions devrait se rapprocher le plus possible de celui du règlement (UE) 2016/679, mais ne devrait pas aller plus loin que celui-ci. Au contraire du règlement cependant, qui prévoit des amendes pouvant se chiffrer à plusieurs millions d'euros, l'avant-projet devrait limiter le montant des amendes à 500 000 francs.

1.6.2 Principales modifications par rapport à l'avant-projet

1.6.2.1 Principales modifications concernant le P-LPD

Le P-LPD a été modifié principalement sur les points suivants:

– Compte tenu des résultats de la consultation externe, la systématique de la loi est retravaillée à plusieurs égards.

– Certaines exceptions du champ d'application du P-LPD sont modifiées. L'exception concernant les traitements effectués lors de procédures devant des tribunaux ou d'autres autorités fédérales juridictionnelles est également remaniée; le P-LPD énumère en outre les autorités fédérales qui ne sont pas soumises à la surveillance du préposé. Enfin, l'exception concernant les registres publics relatifs aux rapports de droit privé a été réintroduite dans une certaine mesure. Le P-LPD prévoit dorénavant que les registres publics relatifs aux rapports de droit privé, notamment l'accès à ces registres et les droits des personnes concernées, sont régis par les dispositions spéciales des lois fédérales applicables.

- La définition du profilage est adaptée à la législation européenne. En outre, une définition pour la violation de la sécurité des données personnelles est ajoutée, car il est ressorti des prises de position reçues lors de la consultation externe qu'elle n'était pas claire.
- La disposition concernant la sécurité des données personnelles est modifiée, car son champ d'application n'était pas clair. La norme concernant les annonces des violations de la sécurité des données personnelles subit également des changements; certaines exceptions sont prévues et il est maintenant assuré que la norme ne viole pas l'interdiction de s'auto-incriminer.
- Une disposition concernant le conseiller à la protection des données personnelles est introduite pour tenir compte des avis exprimés lors de la consultation externe. A certaines conditions, le responsable du traitement pourra être dispensé de procéder à une analyse d'impact relative à la protection des données personnelles.
- Pour tenir compte des critiques de la consultation externe, les recommandations de bonnes pratiques sont remplacées par des codes de conduite, dont l'élaboration appartient aux associations professionnelles et aux associations économiques ainsi qu'aux organes fédéraux uniquement. Ils peuvent les soumettre au préposé, qui doit prendre position et publier ses prises de position. Le préposé, dans le cadre de son activité de conseil, pourra toujours, comme aujourd'hui, élaborer des guides et des outils.
- En lieu et place d'un devoir général de documenter, une disposition sur un registre des activités de traitement est introduite. La consultation externe a montré qu'une obligation de documentation générale était trop floue.
- Les règles relatives aux communications de données personnelles sont en partie remaniées pour tenir compte des résultats de la consultation externe. Le principe selon lequel aucune donnée personnelle ne peut être transmise à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée est supprimé au motif qu'il crée une insécurité juridique par rapport à la systématique de la réglementation. La terminologie relative aux communications de données personnelles à l'étranger moyennant des garanties appropriées est alignée sur celle du règlement (UE) 2016/679. Les exceptions relatives à la communication de données personnelles vers un Etat dont la législation n'assure pas un niveau de protection des données adéquat sont en outre légèrement assouplies. Enfin, seules les obligations d'informer le préposé ou d'obtenir son approbation qui sont exigées par le P-STE 108 sont maintenues.
- La disposition concernant les données d'une personne décédée est reformulée suite à la consultation externe. Elle permet maintenant une pesée globale des intérêts qui peut tenir compte d'un éventuel secret de fonction ou secret professionnel. Compte tenu des résultats de la consulation externe, l'exécuteur testamentaire a été ajouté.

- Les dispositions concernant le devoir d'informer et les exceptions sont précisées. Par ailleurs, le devoir d'informer en cas de décision individuelle automatisée est formulé de manière plus compréhensible et trois exceptions sont insérées.
- Le seuil pour la réalisation d'une analyse d'impact relative à la protection des données personnelles est relevé et des exceptions sont prévues. Suite à la consultation externe, le délai du préposé pour prendre position est raccourci.
- Les dispositions concernant le droit d'accès sont légèrement modifiées suite à la consultation externe. Les exceptions sont désormais explicitement mentionnées, sans qu'elles aient été modifiées dans leur contenu.
- Les cas dans lesquels les traitements de données personnelles effectués par les organes fédéraux doivent reposer sur une base légale prévue par une loi au sens formel ont été modifiés. Contrairement à l'avant-projet, le P-LPD prévoit qu'une base légale au sens formel est exigée lorsque la finalité ou le mode du traitement est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée. L'exigence d'une base légale au sens formel pour le premier cas de figure (finalité du traitement) est nécessaire en raison de l'abrogation de la notion de «profil de la personnalité» et donc de l'exigence d'une base légale au sens formel pour ce type de traitement. Une atteinte grave aux droits fondamentaux de la personne concernée peut également résulter du mode de traitement des données, par exemple dans certains cas les décisions individuelles automatisées. Le projet prévoit par conséquent dans ce cas l'exigence d'une base légale au sens formel. Le niveau de base légale pour les données sensibles et le profilage restent en revanche inchangés par rapport à l'avant-projet.
- Le droit pour la personne d'exiger d'un organe fédéral la limitation d'un traitement de données personnelles la concernant est supprimé. Le P-LPD prévoit dorénavant que la limitation du traitement constitue, pour l'organe fédéral, une mesure de substitution à l'effacement ou à la destruction des données, si certaines conditions sont réalisées.
- Contrairement à l'AP-LPD, qui laisse au préposé la faculté de décider d'ouvrir ou non une enquête, le P-LPD prévoit dorénavant une obligation. Le préposé peut y renoncer uniquement si la violation des prescriptions de protection des données est de peu d'importance.
- Le catalogue des mesures administratives que le préposé est habilité à prononcer est complété. Cette modification ne renforce pas les pouvoirs décisionnels du préposé mais précise uniquement que celui-ci peut également ordonner à un responsable du traitement de respecter certaines obligations, telles que des devoirs d'information ou d'annonce. Enfin, le P-LPD confère au préposé la faculté de prononcer un avertissement si certaines conditions sont remplies, ce qui n'était pas prévu par l'AP-LPD.
- Contrairement à l'AP-LPD, le P-LPD ne prévoit plus que les recours contre les mesures provisoires ordonnées par le préposé n'ont pas d'effet suspensif.

Les dispositions générales de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[56] sont dorénavant applicables.

– La réglementation relative à l'assistance administrative entre le préposé et les autorités étrangères chargées de la protection des données est renforcée.
– Le P-LPD introduit une obligation pour le préposé de percevoir des émoluments auprès des personnes privées pour certaines tâches légales.
– Le régime des sanctions pénales a été retravaillé pour faire suite aux remarques de la consultation externe. La limite maximale de l'amende a été abaissée à 250 000 francs. Le catalogue des comportements punissables a été allégé pour se concentrer sur la violation de devoirs importants incombant au responsable du traitement. La violation du devoir de discrétion redevient une contravention et ne vise plus la communication de données traitées à des fins commerciales. Pour pallier le défaut de punissabilité directe de l'entreprise, le Conseil fédéral prévoit de renforcer la responsabilité des organes dirigeants par l'application de l'art. 6 DPA en plus de l'art. 29 CP. Il propose en outre de punir l'insoumission à une décision du préposé, ce qui permettra d'identifier et de condamner facilement la personne dirigeante responsable, au sein de l'entreprise, de faire exécuter la décision. Cette mesure, associée à la possibilité pour les autorités – déjà présente dans l'avant-projet – de renoncer à poursuivre les personnes physiques responsables et de punir l'entreprise directement, lorsque l'amende ne dépasse pas 50 000 francs et que l'identification de la personne responsable nécessite des actes d'enquête disproportionnés, renforce les possibilités de sanctionner, certes pas les entreprises elles-mêmes, mais leurs dirigeants.
– Le régime transitoire concernant les obligations des responsables du traitement privés est élargi à d'autres devoirs.

1.6.2.2 Principales modifications concernant les autres lois fédérales

Les lois fédérales figurant en annexe du P-LPD sont modifiées principalement sur les points suivants:

– Les bases légales habilitant les organes fédéraux à traiter des profils de la personnalité ont été abrogées ou modifiées.
– Contrairement à l'avant-projet, le projet de loi adapte les dispositions spéciales relatives à la communication de données personnelles à l'étranger au regard des art. 13 et 14 P-LPD afin de garantir une réglementation uniforme en droit fédéral.
– Le projet de loi introduit dans la LOGA un certain nombre de dispositions légales concernant le traitement de données concernant des personnes morales par des organes fédéraux. En effet, en raison de l'abrogation de la pro-

56 RS **172.021**

tection des données des personnes morales, les bases légales prévues par le droit fédéral qui habilitent les organes fédéraux à traiter des données personnelles ne s'appliquent plus lorsque ceux-ci traitent des données concernant des personnes morales. Les art. 5, 13, al. 2, et 36 Cst. sont ainsi respectés.

1.6.2.3 Principales modifications concernant les lois fédérales mettant en œuvre les exigences de la directive (UE) 2016/680

Le nouveau chapitre relatif à la protection des données personnelles introduit dans la loi du 20 mars 1981 sur l'entraide pénale internationale (EIMP)[57] est modifié en partie. Par rapport à l'avant-projet soumis à la consultation externe, le devoir d'information est supprimé car la transparence des traitements des données personnelles est garantie par la loi. En revanche, les droits des personnes concernées font l'objet d'une nouvelle réglementation, d'une part pour mettre en œuvre les exigences de la directive (UE) 2016/680 et d'autre part pour tenir compte de l'exception de l'art. 2, al. 3, P-LPD.

1.6.3 Autres remarques significatives de la consultation externe non retenues

Certains participants demandent que la protection des données en Suisse soit guidée par le principe du «*opt-in*», à savoir que le traitement de données personnelles ne peut se faire que si la personne concernée donne son accord clairement.

Plusieurs participants estiment regrettable que l'AP-LPD ne contienne pas de droit à la portabilité des données, sur le modèle du règlement (UE) 2016/679. Ce droit permet à la personne concernée de récupérer les données qui ont été traitées à son sujet dans un format standard pour se tourner vers un autre fournisseur et assurerait, selon ces participants, un meilleur contrôle des données et favoriserait leur réutilisation et le développement de nouveaux services. A l'inverse, d'autres participants approuvent expressément l'option choisie par le Conseil fédéral, dans la mesure où un tel droit ne vise pas directement la protection de la personnalité et engendrerait des frais importants.

Certains participants souhaitent l'introduction d'un renversement du fardeau de la preuve en faveur de la personne concernée, afin qu'en cas de procédure judiciaire, il appartienne au responsable du traitement de démontrer qu'il traite les données de manière licite. L'absence de renversement du fardeau de la preuve est expressément saluée par quelques participants.

Certains participants regrettent que l'AP-LPD ne prévoie pas de moyens pour les personnes concernées de faire valoir leur droit collectivement. Cette solution est en revanche expressément saluée par d'autres.

57 RS **351.1**

Quelques participants souhaitent que les fichiers de solvabilité soient interdits. Ces fichiers, qui contiennent des informations sur la solvabilité des personnes privées, seraient susceptibles de porter une grave atteinte à la vie privée des gens. En effet, d'une part, les informations que ces fichiers contiennent sont souvent erronées et, d'autre part, la procédure pour demander l'effacement et la suppression des données est souvent peu claire, voire inexistante. D'autres participants demandent que l'on vérifie au moins si un durcissement de la loi en ce qui concerne les entreprises traitant des fichiers de solvabilité ne serait pas opportun. Voir sur ce point le postulat Schwaab 16.3682 «Encadrement des pratiques des sociétés de renseignement de solvabilité», dans le cadre duquel le Conseil fédéral entend examiner l'opportunité d'adopter une législation spécifique régissant les activités des sociétés de renseignements de solvabilité et les solutions légales envisageables.

Certains participants représentant les consommateurs considèrent que la LPD devrait également pouvoir s'appliquer à des entreprises n'ayant pas de siège en Suisse mais qui procèdent à des traitements ayant des effets en Suisse. Ces entreprises devraient notamment avoir un représentant en Suisse.

Différents participants estiment qu'un droit à l'oubli devrait être prévu. Il s'agit là d'un aspect important du droit européen qui fait défaut dans l'AP-LPD. D'autres participants approuvent au contraire que l'AP-LPD ne mentionne pas expressément ce droit, qui peut déjà être déduit des règles actuelles.

1.6.4 Evaluation du projet de loi

Le projet remplace la LPD de 1992 afin, d'une part, de mieux répondre aux défis liés aux nouvelles technologies et, d'autre part, de tenir compte des exigences du droit européen. Il reprend dans la mesure du possible les règles et principes qui ont fait leurs preuves. Il ne crée pas de nouvelle compétence en faveur de la Confédération, si bien que les cantons restent souverains, sous réserve des exigences européennes et de dispositions fédérales matérielles sectorielles, pour les traitements de données par les organes cantonaux. Le projet modernise la terminologie, encourage l'autorégulation, renforce les obligations des responsables du traitement et les droits des personnes concernées, confère de nouveaux pouvoirs au préposé et renforce les aspects pénaux de la loi. Ces modifications créent un cadre juridique plus clair, compatible avec les besoins de l'innovation, et permettant à la Suisse de rester concurrentielle au plan international.

Le projet révise aussi partiellement les lois spécifiques au domaine de la coopération Schengen. Il s'agit pour la Suisse de satisfaire aux engagements pris vis-à-vis de l'Union européenne.

Le choix d'une proposition globale, comprenant une révision totale de la LPD et la modification de nombreuses autres lois fédérales, s'est imposé car il aurait été très compliqué de mettre en œuvre certaines exigences de la directive (UE) 2016/680 pour certains traitements uniquement (pouvoirs de décision du préposé, par ex.). L'option choisie permet au surplus d'établir une législation cohérente, mettant en place un cadre général de protection des données clair et applicable le plus largement possible.

1.7 Autres mesures examinées

Dans le cadre de ses travaux, le Conseil fédéral a examiné d'autres mesures, mais il a finalement décidé de ne pas les prévoir dans le projet. Certaines de ces mesures ont aussi été proposées lors de la consultation externe (cf. ch. 1.6.3). Il s'agit principalement des suivantes:

1.7.1 Ediction de règles de protection des données contraignantes par le préposé

L'option de charger le préposé d'édicter des règles contraignantes a été écartée au stade de l'avant-projet. Certes, cette solution aurait eu le mérite de permettre au préposé d'obliger directement les destinataires des règles en question à les appliquer. Elle aurait toutefois soulevé bon nombre de problèmes en lien avec le principe de la légalité (délégation de compétence au préposé, densité normative). Par ailleurs, par rapport à la solution retenue par l'avant-projet de loi soumis à la consultation externe, à savoir des recommandations de bonnes pratiques, le processus d'adoption aurait été plus lent, dans la mesure où l'on aurait dû suivre le processus législatif applicable aux ordonnances de l'administration fédérale. Par ailleurs, cette option aurait laissé peu de marge de manœuvre aux milieux concernés, ce qui peut nuire à l'acceptation de ces règles.

1.7.2 Renversement du fardeau de la preuve

Le Conseil fédéral a examiné l'opportunité de prévoir un renversement du fardeau de la preuve, sur le modèle l'art. 13*a* de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale (LCD)[58]. Cette solution permet au juge, dans un cas concret, et lorsque cela paraît justifié au vu des intérêts des parties à la procédure, d'exiger de la personne qui traite des données la preuve que le traitement est conforme aux prescriptions légales en la matière. Or, les tribunaux civils sont déjà aujourd'hui en position, dans le cadre de la libre appréciation des preuves et de l'obligation des parties de collaborer, de résoudre les problèmes liés à l'établissement des preuves. La consultation menée à propos de la loi sur les services financiers a par ailleurs montré que les propositions de renversement du fardeau de la preuve se heurtent à de fortes résistances[59]. Le préposé aurait voulu qu'une telle solution soit prévue.

58 RS **241**
59 Voir le message du Conseil fédéral du 4 novembre 2015 concernant la loi sur les services financiers (LSFin) et la loi sur les établissements financiers (LEFin), FF **2015** 8101.

1.7.3 Exercice collectif des droits

Le Conseil fédéral est en train d'élaborer, dans le cadre de la réalisation de la motion 13.3931 Birrer-Heimo, un avant-projet de loi destiné à faciliter l'exercice collectif des droits. Cet avant-projet s'appliquera au domaine privé de manière générale, et donc aussi à la protection des données. Le Conseil fédéral estime qu'il n'est pas opportun de prévoir un régime spécial, en introduisant dans la LPD un système d'exercice collectif des droits (tel que, par exemple, l'extension du droit d'action des organisations et l'institution d'actions de groupe ou de transactions de groupes[60]).

1.7.4 Droit à la portabilité des données

La question d'introduire un droit à la portabilité des données pour les personnes concernées, tel que prévu par l'art. 20 du règlement (UE) 2016/679, a été examinée. Le droit à la portabilité des données permet à la personne concernée de transmettre ses données d'un système de traitement automatisé à un autre. Il implique que la personne reçoive les données qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine. Le Conseil fédéral estime que ce droit vise plus à permettre aux personnes concernées de réutiliser leurs données afin de faire jouer la concurrence, qu'à protéger leur personnalité. La mise en œuvre de ce droit paraît par ailleurs problématique, dans la mesure où elle suppose une concertation des responsables du traitement et sans doute un accord – au moins implicite – sur les supports et standards informatiques utilisés. L'analyse d'impact de la réglementation a au surplus montré que l'introduction d'un tel droit pourrait être très coûteuse, particulièrement pour les entreprises qui comptent plus de 50 employés, qui devraient engager du personnel supplémentaire.

Le Conseil fédéral juge opportun d'attendre les résultats des expériences au sein de l'Union européenne avant d'envisager d'introduire un droit à la portabilité des données en Suisse. Il poursuivra son examen dans le cadre de la Stratégie «Suisse numérique». Le préposé aurait souhaité qu'un droit à la portabilité soit introduit dans le projet.

1.7.5 Commission extra-parlementaire pour l'élaboration et l'approbation des recommandations de bonnes pratiques

Il a été envisagé de confier la tâche d'élaborer et d'approuver des recommandations de bonnes pratiques à une commission extra-parlementaire. Cette solution a été écartée au stade de l'avant-projet, au motif qu'elle engendrerait des charges administratives et financières supplémentaires et serait plus bureaucratique.

60 Voir les art. 101 ss de l'avant-projet LSFin.

1.7.6 Modification de l'organisation de l'autorité de contrôle

Il a été envisagé de modifier l'organisation du préposé et d'en faire une autorité collégiale. Il a finalement été décidé de conserver la structure actuelle, qui est peu bureaucratique, simple, garantit des prises de décisions rapides ainsi qu'une bonne circulation des informations et qui est bien représentée au niveau des cantons, ainsi que dans de nombreux pays européens (Allemagne, Espagne ou Pologne).

1.7.7 Mise en place de mécanismes spéciaux de gestion des conflits

Le Conseil fédéral a examiné l'opportunité de créer un organe chargé de régler les conflits de protection des données de manière extra-judiciaire. Il y a renoncé, dans la mesure où un tel mécanisme existe déjà dans de nombreux domaines (Ombudscom, Ombudsman des banques, de l'assurance-privée et de la SUVA, etc.) et que cela entraînerait des conflits de compétences. Par ailleurs, la création d'un organe rattaché au préposé occasionnerait des coûts très importants.

1.8 Analyse d'impact de la réglementation

L'analyse d'impact de la réglementation (AIR) est un outil permettant d'examiner et de présenter les impacts économiques des projets législatifs de la Confédération. Cet instrument est obligatoire et est en particulier important dans le cas de messages, de rapports explicatifs et de propositions au Conseil fédéral. Les bases juridiques de l'AIR se trouvent aux art. 170 Cst. et 141, al. 2, de la loi du 13 décembre 2002 sur l'Assemblée fédérale (LParl)[61].

L'OFJ et le Secrétariat d'Etat à l'économie (SECO) ont mandaté l'entreprise PwC pour qu'elle procède à une AIR[62] concernant l'avant-projet. L'analyse avait pour but de servir de base pour l'évaluation de ce dernier. Dans la mesure où le projet reprend la plupart des mesures examinées, les considérations concernant l'avant-projet peuvent également être appliquées au projet. L'analyse est principalement basée sur les résultats d'une enquête en ligne auprès d'entreprises ainsi que sur des entretiens effectués avec des professionnels et des experts de la protection des données. Dans le cadre de l'enquête, l'avant-projet a été dans l'ensemble très bien accueilli.

L'AIR comprend cinq points à examiner: la nécessité et la possibilité d'une intervention de l'Etat; l'impact du projet sur les différents groupes de la société; les implications pour l'économie dans son ensemble; les autres réglementations entrant en ligne de compte; les aspects pratiques de l'exécution.

61 RS **171.10**
62 Cette AIR est disponible sur le site Internet de l'OFJ: www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html.

1.8.1 Nécessité et possibilité d'une intervention de l'Etat

La nécessité de légiférer est d'une part fondée sur les importantes évolutions technologiques et sociales de ces dernières années, qui soulèvent des craintes au sein de la population et qui ont entraîné de nouvelles menaces pour la protection des données. A cet égard, l'AP, comme le projet, visait principalement à améliorer le contrôle et la maîtrise sur les données, et à renforcer la transparence des traitements. La nécessité d'intervenir de la Confédération découle d'autre part des évolutions du droit au niveau international, en particulier le P-STE 108 et, pour les secteurs touchant à la coopération Schengen, la directive (UE) 2016/680. Le règlement (UE) 2016/679 doit aussi être pris en considération.

1.8.2 Impact du projet sur les différents groupes de la société

Les modifications envisagées par l'AP concernaient toutes les entreprises actives en Suisse. PwC a classé ces dernières d'après leur «exposition au droit de la protection des données», matérialisée par branche et par taille. Les segments suivants ont été distingués:

- segment A: entreprises faiblement exposées au droit sur la protection des données;
- segment B: entreprises moyennement exposées au droit sur la protection des données;
- segment C: entreprises fortement exposées au droit sur la protection des données.

L'application de la segmentation pour les branches économiques suisses sélectionnées implique qu'environ 335 000 entreprises (55,1 %) sont classées dans le segment A, environ 265 000 dans le segment B (43,5 %) et près de 8000 dans le segment C (1,4 %).

Les résultats de l'analyse ont montré que les entreprises du segment A étaient généralement peu touchées par les mesures prévues dans le cadre de l'AP. Certains experts ont toutefois fait valoir lors des discussions que les entreprises du segment A seraient plus affectées par les mesures de l'AP que les grandes entreprises, dans la mesure où elles ne disposent souvent pas de service de mise en conformité, ce qu'il faudrait compenser par des coûts additionnels. En revanche, en raison de leurs activités, de leur taille et de leur ouverture vers l'étranger, les entreprises des segments B et C sont affectées de manière plus significative[63].

63 Pour une vision détaillée des impacts pour chaque mesure, voir le tableau récapitulatif aux pages 54 à 58 de l'AIR.

1.8.3 Implications pour l'économie dans son ensemble

Il convient de distinguer les effets sur l'économie de ceux sur la société dans son ensemble. Pour l'économie, la discussion sur les effets supposés a principalement porté sur la problématique de la concurrence. Sur le plan international, il faut s'attendre pour la Suisse à de graves désavantages concurrentiels par rapport aux Etats membres de l'Union européenne, si elle perdait son statut de pays doté d'un niveau adéquat de protection des données ou si elle adoptait des réglementations qui lui seraient propres ou qui seraient plus restrictives que le droit de l'Union européenne.

Dans la mesure où les entreprises d'un segment donné sont toutes concernées de manière égale, les modifications envisagées sont considérées, au plan suisse, comme neutre au niveau de la concurrence. En revanche, selon l'AIR, la question de savoir dans quelle mesure une protection renforcée des données amènera un avantage concurrentiel au niveau international reste ouverte.

Du point de vue de l'impact sur la société, aucune obligation *per se* pour les personnes concernées n'est prévue. Les experts interrogés pensent que les mesures examinées dans le cadre de l'AIR sont appropriées pour faciliter, au moins de façon formelle, l'exercice de leurs droits par les personnes concernées. Ils se réfèrent principalement au renforcement du droit d'accès, à l'amélioration de la transparence des traitements, aux améliorations concernant les droits des personnes concernées, ainsi qu'à l'introduction d'un droit à la portabilité des données, à laquelle le Conseil fédéral a renoncé pour le moment (ch. 1.7.4). La question de savoir si les personnes concernées profiteront concrètement des mesures examinées dépendra surtout de l'importance qu'elles accordent à la protection de leurs données personnelles. Dans ce contexte, le paramétrage par défaut favorable au respect de la vie privée (*privacy by default*) peut devenir un instrument important de la protection des données.

1.8.4 Autres réglementations entrant en ligne de compte

Dans le cadre des discussions avec les experts, d'autres solutions que les mesures prévues ont été évoquées, telles le fait de soumettre les données aux règles des droits réels. Ces solutions ont toutefois souvent été jugées inapplicables car s'écartant trop des évolutions sur le plan international (aucun autre pays européen, par exemple, ne prévoit de propriété sur les données). Pour la concurrence internationale, il est suggéré de renoncer aux mesures plus contraignantes que celles prévues dans les pays de l'Union européenne et d'éviter ainsi une surrégulation. L'option de nommer une commission d'experts chargée d'édicter des recommandations de bonnes pratiques, à laquelle le Conseil fédéral a renoncé depuis, a été saluée car elle permet de s'adapter rapidement aux nouveautés technologiques (ch. 1.7.5).

1.8.5 Aspects pratiques de l'exécution

Pour limiter les coûts liés à la mise en œuvre des mesures, une majorité des professionnels interrogés recommande que l'on permette aux entreprises de se conformer aux obligations d'information de façon standardisée. Cela pourrait selon eux s'effectuer par exemple au moyen d'explications relatives au droit de la protection des données ou par la pose de pictogrammes, sur un site Internet ou dans des conditions générales. En cas d'obligations d'information «individualisées», les professionnels s'attendent à des coûts considérables.

Dans un objectif de sécurité juridique et de transparence, le projet de loi devrait faire usage de concepts clairement définis (définitions légales) et désigner précisément les faits qui font naître une obligation. Il faudrait indiquer, par exemple, dans quels cas il convient de réaliser une analyse d'impact relative à la protection des données. Pour améliorer la prise de conscience concernant les problèmes posés par la protection des données et faciliter la mise en œuvre de la loi, on signale la nécessité d'une communication ciblée (par ex. avec des notices, brochures) et le développement de guides: ces mesures pourraient en particulier profiter aux entreprises peu exposées au droit de la protection des données. L'idée de créer une commission d'experts indépendante a été dans ce contexte accueillie favorablement par la majorité des experts (ch. 1.7.5).

2 Directive (UE) 2016/680

2.1 Présentation de la directive (UE) 2016/680

2.1.1 Déroulement des négociations

Les délibérations des Etats membres de l'Union européenne et des quatre Etats associés à la coopération Schengen (la Norvège, l'Islande, la Suisse et le Liechtenstein dans le cadre de leurs droits de participation) ont eu lieu au sein des groupes de travail du Conseil de l'Union européenne (comités mixtes) compétents en la matière, au cours des années 2012 à 2015, sous la présidence de l'Etat membre de l'Union européenne respectif qui détenait la présidence au sein de l'Union. Des représentants de la Confédération et des cantons ont participé aux travaux d'élaboration de la directive (UE) 2016/680, dans le cadre de ces comités mixtes. Le 27 avril 2016, le Parlement européen et le Conseil de l'Union européenne ont formellement adopté la directive (UE) 2016/680.

2.1.2 Aperçu

La directive (UE) 2016/680 vise à protéger les données à caractère personnel traitées 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cet acte a pour objectif de garantir un niveau élevé de protection des données des personnes physiques tout en facilitant l'échange de ces données entre les autori-

tés compétentes des différents Etats Schengen. Contrairement à la décision-cadre 2008/977/JAI, la directive (UE) 2016/680 s'applique aussi bien aux traitements transfrontières de données qu'aux traitements effectués par les autorités policières et judiciaires au niveau strictement national. Son texte est aligné sur celui du règlement (UE) 2016/679 (voir ci-après ch. 4) pour que, dans les grandes lignes, les mêmes principes généraux s'appliquent. Certains aménagements sont toutefois prévus afin de trouver un juste équilibre entre le droit de la personne concernée à la protection de sa sphère privée et les besoins des autorités pénales. Les principales innovations sont présentées ci-après.

La directive (UE) 2016/680 introduit une obligation d'établir une distinction entre les différentes catégories de personnes concernées (art. 6) ainsi que des règles sur la distinction des données et la vérification de la qualité de celles-ci. L'art. 8 règle la licéité du traitement. Les traitements doivent en substance reposer sur une base légale. D'autres motifs justificatifs, par exemple le consentement de la personne concernée, ne sont pas applicables pour les traitements tombant dans le champ d'application de la directive (UE) 2016/680. L'art. 11 pose le principe selon lequel toute décision fondée exclusivement sur un traitement automatisé est interdite, à moins qu'elle ne soit autorisée par la législation nationale et que le droit pour la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement soit garanti.

Le chapitre III règle les droits de la personne concernée. L'art. 16, par. 3, prescrit qu'au lieu de procéder à l'effacement, le responsable du traitement est tenu de limiter le traitement lorsque l'exactitude des données est contestée par la personne concernée et qu'elle ne peut pas être déterminée. L'art. 17 dispose qu'en cas de restriction, la personne concernée doit pouvoir exercer ses droits par l'intermédiaire de l'autorité de contrôle. L'art. 18 prévoit en outre que les Etats Schengen peuvent prévoir que les droits prévus aux art. 13, 14 et 16 sont exercés conformément au droit de procédure de l'Etat Schengen lorsque les données figurent dans une décision ou un dossier judiciaire faisant l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale.

Le chapitre IV règle les obligations du responsable du traitement et du sous-traitant. Il introduit le principe de protection des données dès la conception et par défaut (art. 19 et 20). L'art. 24 prévoit quant à lui une obligation pour le responsable du traitement et le sous-traitant de tenir un registre de toutes les catégories d'activités de traitement effectuées sous leur responsabilité. Les responsables du traitement sont tenus d'autre part d'effectuer une analyse d'impact relative à la protection des données préalablement à certains traitements (art. 27) et de consulter le cas échéant l'autorité de contrôle (art. 28). Les art. 30 et 31 introduisent une obligation pour le responsable du traitement d'annoncer certains cas de violation des données à l'autorité de contrôle et le cas échéant à la personne concernée.

Le chapitre V règle le transfert de données vers des pays tiers ou à des organisations internationales. La Commission européenne est chargée d'évaluer le niveau de protection assuré par un territoire ou un secteur de traitement dans un pays tiers (art. 36). Lorsque la Commission européenne n'a pas constaté par voie de décision le caractère adéquat du niveau de protection dans l'Etat tiers, le transfert de données peut néanmoins avoir lieu lorsque des garanties appropriées ont été fournies (art. 37)

ou par dérogations dans des situations particulières (art. 38). L'art. 39 de la directive (UE) 2016/680 règle quant à lui le transfert de données à caractère personnel à des destinataires établis dans des Etats tiers, lorsque des données ne peuvent pas être transmises aux autorités compétentes par les canaux habituels de la coopération policière ou judiciaire.

Le chapitre VI oblige les Etats Schengen à instituer des autorités de contrôle indépendantes en matière de protection des données. Les art. 45 à 47 règlent les compétences, les missions et les pouvoirs des autorités de contrôle. En vertu de l'art. 45, par. 2, les Etats Schengen prévoient que l'autorité de contrôle n'est pas compétente pour contrôler les traitements effectués par les juridictions dans l'exercice de leur fonction juridictionnelle. En vertu de l'art. 45, par. 2, les Etats Schengen peuvent également prévoir une exception pour les traitements des données effectués par d'autres autorités judiciaires indépendantes lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle. Il peut s'agir par exemple du ministère public. L'art. 47, par. 1, oblige les Etats Schengen à prévoir que l'autorité de contrôle doit être dotée de pouvoirs d'enquête effectifs, soit au moins d'obtenir du responsable du traitement ou du sous-traitant l'accès aux données traitées et à toute information nécessaire à l'accomplissement de ses tâches. En vertu du par. 2, l'autorité de contrôle doit également disposer de pouvoirs effectifs en matière d'adoption de mesures correctrices, telles que par exemple le pouvoir d'adresser un avertissement à un responsable du traitement ou à un sous-traitant, d'ordonner la mise en conformité des traitements le cas échéant par une rectification ou un effacement des données ainsi que d'ordonner la limitation temporaire ou définitive du traitement, y compris son interdiction. Les pouvoirs de l'autorité de contrôle ne doivent toutefois pas interférer avec les règles spécifiques à la procédure pénale, y compris pour les enquêtes et les poursuites concernant les infractions pénales, ni avec l'indépendance du pouvoir judiciaire. Le chapitre VII porte sur les voies de recours, la responsabilité et les sanctions. L'art. 52 prescrit que la personne concernée a le droit d'introduire une réclamation auprès de l'autorité de contrôle. En vertu de l'art. 53, la personne concernée a également le droit de former un recours juridictionnel effectif contre une décision de l'autorité de contrôle la concernant. L'art. 55 prévoit en outre un droit pour les personnes concernées de se faire représenter à certains conditions.

2.2 Reprise de la directive (UE) 2016/680 en tant que développement de l'acquis de Schengen

En vertu de l'art. 2, par. 3, de l'accord d'association à Schengen, la Suisse s'est engagée en principe à accepter, à mettre en œuvre et à appliquer tout développement de l'acquis de Schengen. La directive (UE) 2016/680 constitue un développement de l'acquis de Schengen. Comme on le verra sous ch. 2.4, la reprise de la directive (UE) 2016/680 implique l'adoption d'un certain nombre de mesures législatives au niveau fédéral, car le droit en vigueur ne remplit pas toutes les exigences de cet acte.

Conformément à l'accord d'association, la Suisse doit se prononcer sur l'acceptation de chaque acte qui lui a été notifié comme développement de l'acquis de Schengen

et, le cas échéant, sur sa transposition dans son ordre juridique interne, dans un délai de 30 jours à compter de la date d'adoption dudit acte (art. 7, par. 2, let. a, AAS).

Lorsque l'acte à reprendre a une portée juridique contraignante, la notification de l'Union européenne et la note de réponse de la Suisse constituent un échange de notes ayant pour la Suisse valeur de traité international. Conformément aux dispositions constitutionnelles, ce traité doit être conclu soit directement par le Conseil fédéral, soit après approbation par l'Assemblée fédérale et, en cas de référendum, par le peuple.

Le Parlement européen et le Conseil de l'Union européenne ont adopté la directive (UE) 2016/680 le 27 avril 2016. Cet acte n'a toutefois été notifié à la Suisse que le 1er août 2016 mettant ainsi cette dernière dans l'impossibilité d'adresser sa note de réponse au Secrétariat général du Conseil dans le délai prescrit par l'accord d'association. La Suisse n'a pu transmettre sa note de réponse que le 1er septembre 2016.

Dans le cas d'espèce, l'Assemblée fédérale est compétente pour approuver l'échange de notes concernant la reprise de la directive (UE) 2016/680. Vu que la directive ne peut lier la Suisse qu'après l'accomplissement de ses exigences constitutionnelles, le Conseil fédéral en a informé l'Union européenne dans sa réponse du 1er septembre 2016 (art. 7, par. 2, let. b, AAS).

La Suisse dispose d'un délai maximal de deux ans, à compter de la date de la notification par l'Union européenne, pour reprendre l'acte en question dans son ordre juridique (y compris le cas échéant la procédure référendaire). Une fois la procédure interne d'approbation achevée, la Suisse doit notifier sans délai et par écrit aux institutions européennes compétentes que toutes les exigences constitutionnelles ont été accomplies, ce qui correspond à une ratification de l'échange de notes conclu entre la Suisse et l'Union européenne. L'échange de notes concernant la reprise de la directive (UE) 2016/680 entrera en vigueur le jour de la communication de la Suisse. La directive (UE) 2016/680 a été notifiée à la Suisse le 1er août 2016. Par conséquent, le délai maximal pour la reprise et la mise en œuvre de cet acte prend fin le 1er août 2018.

2.3 Choix légistique

La directive (UE) 2016/680 n'est directement applicable ni pour les Etat membres de l'Union européenne, ni pour la Suisse. Elle doit être reprise dans les différents droits nationaux. Cela implique, pour la Suisse, d'adapter certaines lois fédérales.

En tant qu'Etat associé à Schengen, la Suisse n'est en principe tenue d'appliquer la directive (UE) 2016/680 que dans la mesure où les traitements s'inscrivent dans le cadre de la coopération instaurée par Schengen dans le domaine pénal. Une transposition limitée à ce domaine serait en principe suffisante. Toutefois, vu que le contenu de la directive (UE) 2016/680 correspond pour une grande partie à celui du P-STE 108 tout en étant plus détaillé, le Conseil fédéral propose une transposition plus étendue des exigences de la directive (UE) 2016/680 selon les critères suivants:

– Les dispositions de la directive (UE) 2016/680 qui correspondent aux exigences du P-STE 108 sont transposées dans le P-LPD et s'appliquent à l'en-

semble des traitements de données effectués par les personnes privées et les organes fédéraux.

– Les exigences de la directive (UE) 2016/680 qui correspondent à des principes généraux de protection des données sans toutefois être prévus par le P-STE 108 sont transposées à l'ensemble des traitements de données effectués par les organes fédéraux, afin d'éviter des niveaux de protection des données différents dans le secteur public.
– Les exigences de la directive (UE) 2016/680 relatives à l'autorité de contrôle en matière de protection des données sont transposées dans le P-LPD. Certaines de ces exigences sont également prévues par le P-STE 108. Au niveau fédéral, le préposé est l'autorité de contrôle nationale compétente pour l'ensemble des règles fédérales de protection des données. La réglementation applicable au préposé doit être réglée de manière uniforme, indépendamment du domaine de surveillance concerné.
– Les exigences de la directive (UE) 2016/680 qui constituent des normes spécifiques à la coopération instaurée par Schengen dans le domaine pénal sont transposées uniquement dans les législations applicables à ces domaines (cf. ch. 9.3).

2.4 Principales modifications législatives nécessaires

La reprise de la directive (UE) 2016/680 implique, outre des modifications de la LPD, celles d'autres lois fédérales: CP, le code de procédure pénale du 5 octobre 2007 (CPP)[64], EIMP, la loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale[65], la loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[66], la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats[67], la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[68] et la loi du 12 juin 2009 sur l'échange d'informations Schengen (LEIS)[69]. Les dispositions de la directive (UE) 2016/680 qui doivent être transposées dans le P-LPD et dans les lois sectorielles susmentionnées sont indiquées dans le commentaire des dispositions légales.

On constate que différentes lois fédérales applicables au domaine de la police contiennent des dispositions de protection des données. On peut se demander si cette dispersion de normes ne complique pas l'application du droit, et s'il ne faudrait pas réfléchir à l'élaboration d'une loi fédérale régissant l'ensemble des activités de police, comme cela existe dans de nombreux cantons.

64 RS **312**
65 RS **351.6**
66 RS **351.93**
67 RS **360**
68 RS **361**
69 RS **362.2**

3 P-STE 108

3.1 Aperçu

Les Etat parties sont tenus d'appliquer le projet de modernisation à l'ensemble des traitements relevant de leur juridiction dans les secteurs public et privé. Seuls les traitements effectués par une personne dans le cadre de ses activités personnelles ne sont pas régis par le projet de modernisation (art. 3).

En vertu du P-STE 108, les obligations du responsable du traitement doivent être étendues. Ainsi, celui-ci est tenu d'annoncer à l'autorité de contrôle compétente certains cas de violation de la protection des données (art. 7, par. 2). Son devoir d'informer la personne concernée doit en outre être étendu, notamment par rapport aux informations à fournir et en cas de décision individuelle automatisée. Les Etats parties doivent également prévoir une obligation pour le responsable du traitement d'effectuer une analyse d'impact préalablement à certains traitements et d'appliquer les principes de la protection des données dès la conception et par défaut (art. 8bis, par. 2 et 3).

Les Etats parties doivent conférer à la personne concernée le droit de ne pas être soumise à une décision prise uniquement sur le fondement d'un traitement automatisé de ses données, sans qu'elle puisse faire valoir son point de vue (art. 8, let. a). Son droit d'accès doit également être étendu (art. 8, let. b) et les conditions applicables au consentement de la personne concernée, renforcées.

Les Etats parties sont tenus d'établir un régime de sanctions et un système de recours (art. 10).

Le principe de base selon lequel des données ne peuvent être transférées à un Etat tiers que si un niveau approprié de protection est garanti reste le même que dans la convention STE 108 actuelle. Selon le projet de modernisation (art. 12), un niveau de protection approprié peut être garanti par les règles de droit de l'Etat ou de l'organisation internationale destinataire ou moyennant certaines garanties. En l'absence d'un niveau de protection approprié, des données peuvent être transférées vers un Etat tiers si la personne concernée y a valablement consenti ou dans d'autres cas exceptionnels. Enfin, le projet de modernisation oblige les Etats parties à prévoir que l'autorité de contrôle peut exiger de la personne qui transfère les données de démontrer l'effectivité des garanties prises et est habilitée, le cas échéant, à interdire ou à suspendre le transfert des données.

Les Etats parties sont tenus d'instituer une autorité de contrôle indépendante, comme l'exige du reste la convention STE 108. En vertu du projet de modernisation (art. 12bis), les autorités de contrôle doivent être habilitées à rendre des décisions contraignantes susceptibles de recours et à prononcer des sanctions administratives. Seuls les traitements effectués par des organes dans l'exercice de leurs fonctions juridictionnelles sont soustraits de la surveillance de l'autorité de contrôle. L'autorité de contrôle doit également avoir pour mission de sensibiliser le public et les responsables du traitement.

3.2 Ratification du protocole d'amendement à la convention STE 108

Le P-STE 108 a vocation à devenir un instrument universel. En effet, la convention actuelle est déjà ouverte à la ratification d'Etats non membres du Conseil de l'Europe. Une cinquantaine d'Etats ont ratifié le texte actuel, dont quatre Etats qui ne sont pas membres du Conseil de l'Europe (Uruguay, Maurice, Sénégal, Tunisie); plusieurs autres Etats non membres du Conseil de l'Europe sont également en passe de la ratifier (Maroc, Cap Vert, Burkina Faso, Argentine). L'intérêt d'Etats extra-européens à ratifier le P-STE 108 pourrait s'accroître du fait que la ratification de cet instrument sera considérée par l'Union européenne comme un critère déterminant pour l'obtention d'une décision d'adéquation.

Le projet de modernisation permet d'harmoniser et de renforcer le niveau de protection des données au plan international, ce qui renforcera aussi la protection dont bénéficient les citoyens suisses lorsque leurs données personnelles font l'objet de traitements transfrontières. Le projet contribue également à faciliter les flux transfrontières de données entre les Etats parties, ce qui permet un accès facilité au marché de ces pays pour les entreprises suisses. La ratification du protocole d'amendement de la convention STE 108 sera un critère central pour l'Union européenne lorsqu'elle aura à décider du maintien de la décision d'adéquation en faveur de la Suisse, qui elle seule peut lui garantir le libre accès au marché européen.

Ainsi, que ce soit pour des raisons tenant à la protection des droits de l'homme ou pour des raisons économiques (faciliter les flux transfrontières), la Suisse a intérêt à ratifier rapidement le protocole d'amendement à la convention STE 108. On notera à cet égard que le Conseil fédéral, dans plusieurs réponses à des interventions parlementaires, a montré son soutien au P-STE 108 et qu'il s'est par ailleurs engagé pour un renforcement de la protection des données dans le cadre de son action en faveur des droits de l'homme[70]. Enfin, il convient de relever que les mesures prévues par le P-STE 108 convergent avec les objectifs annoncés par le Conseil fédéral dans sa décision du 9 décembre 2011 sur la base des résultats de l'évaluation de la LPD[71].

L'art. 4 du P-STE 108 oblige chaque Etat partie à prendre, dans son droit interne, les mesures nécessaires pour donner effet aux dispositions de cet acte. Ces mesures doivent de plus entrer en vigueur au moment de la ratification ou de l'adhésion à la future convention STE 108. Les Etats parties n'ont pas la faculté de formuler des réserves (art. 25).

Le contenu du P-LPD est pleinement conforme aux exigences du protocole d'amendement, de sorte que, le moment venu, une ratification de ce protocole sera possible sans nouvelle modification de la législation suisse.

70 Le Conseil fédéral a notamment déclaré soutenir les travaux en cours au niveau du Conseil de l'Europe dans sa réponse aux interventions parlementaires suivantes: Ip. Eichenberger 13.4209 («US-Swiss Safe Harbor Framework. Restauration de la confiance dans le cadre de l'échange de renseignements avec les Etats-Unis»); Qst. Gross 13.1072 («Pacte de l'ONU relatif aux droits civils et politiques. Intégration de la protection des données»).

71 FF **2012** 255

3.3 Principales modifications législatives nécessaires

Les dispositions du P-STE 108 ne sont pas directement applicables. En vue de ratifier le protocole d'amendement de cet acte, la Suisse doit adapter certaines dispositions de droit fédéral. Les dispositions du projet de modernisation qui doivent être transposées dans le P-LPD sont indiquées dans le commentaire des dispositions de cet acte.

4 Règlement (UE) 2016/679 sur la protection des données à caractère personnel

4.1 Aperçu

Le règlement (UE) 2016/679 est le texte fondamental en matière de protection des données au niveau de l'Union européenne. La directive (UE) 2016/680 s'en inspire largement, au point que les deux textes contiennent un régime très analogue. Le règlement est cependant plus détaillé, et la directive contient des particularités propres au domaine pénal. Le règlement (UE) 2016/679 ne fait pas partie de l'acquis de Schengen.

Le règlement (UE) 2016/679 règle principalement la protection des données traitées dans le cadre du marché intérieur, mais s'applique aussi au secteur public. Il établit les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données (art. 1).

Le chapitre III règle les droits des personnes concernées. Par rapport à la directive 95/46/CE, ces droits sont renforcés. Ainsi, le règlement (UE) 2016/679 garantit aux personnes concernées un meilleur accès aux données (art. 12 à 15). Cet acte leur confère en outre un droit à la rectification (art. 16), un droit à l'effacement (art. 17) également appelé «droit à l'oubli», ainsi qu'un droit à la limitation du traitement (art. 18). Les personnes concernées disposent également d'un droit à la portabilité des données d'un prestataire de services à un autre (art. 20). Enfin, elles ont le droit de s'opposer à un traitement, notamment à des fins de profilage (art. 21), et à ne pas faire l'objet d'une décision individuelle automatisée (art. 22).

Le chapitre IV règle les obligations du responsable du traitement et du sous-traitant. Il introduit le principe de protection des données dès la conception et par défaut (art. 25). Il définit les conditions applicables à la sous-traitance (art. 28 et 29). Les responsables du traitement ont également l'obligation, dans certains cas, d'annoncer les violations de données à caractère personnel à l'autorité de contrôle et à la personne concernée (art. 33 et 34). Les responsables du traitement sont tenus d'effectuer une analyse d'impact relative à la protection des données préalablement à certains traitements (art. 35) et de consulter le cas échéant l'autorité de contrôle (art. 36). En outre, les pouvoirs publics et les entreprises qui effectuent des traitements de données présentant des risques doivent désigner un délégué à la protection des données (art. 37 à 39). Enfin, les Etats membres de l'Union européenne doivent encourager l'élaboration de codes de conduite destinés à contribuer à la bonne application du

règlement (UE) 2016/679 (art. 40 et 41) et mettre en place des mécanismes de certification en matière de protection des données (art. 42 et 43).

Le chapitre V du règlement (UE) 2016/679 règle le transfert de données vers des Etat tiers ou à des organisations internationales. La Commission européenne est chargée d'évaluer le niveau de protection assuré par un territoire ou un secteur de traitement dans un pays tiers (art. 45). Lorsque la Commission européenne n'a pas constaté par voie de décision le caractère adéquat du niveau de protection sur un territoire ou dans un secteur, le transfert de données peut néanmoins avoir lieu lorsque des garanties appropriées ont été fournies (art. 46), au moyen de règles d'entreprise contraignantes (art. 47) ou par dérogation dans des situations particulières (art. 49).

Le chapitre VI porte sur les autorités de contrôle indépendantes. Les Etats membres ont la faculté d'instituer une ou plusieurs autorités de contrôle chargées de surveiller l'application du règlement (UE) 2016/679 et, le cas échéant, également de la directive (UE) 2016/680. Les exigences applicables au statut d'indépendance de l'autorité de contrôle sont identiques dans les deux actes. Chaque autorité de contrôle doit disposer de certains pouvoirs d'enquête (art. 58, par. 1). Elle est habilitée à adopter les mesures correctrices prévues par le règlement (UE) 2016/679 (par. 2).

Le chapitre VII instaure des mécanismes visant à assurer une application cohérente de la législation en matière de protection des données dans l'ensemble de l'Union européenne. En particulier, dans des affaires transfrontières faisant intervenir plusieurs autorités de contrôle nationales, une décision de contrôle unique sera prise. Ce principe, connu sous le nom de «guichet unique», permet à une entreprise ayant des filiales dans plusieurs Etats membres de n'avoir à traiter qu'avec l'autorité de contrôle de l'Etat-membre dans lequel elle a son établissement principal. Cette autorité est désignée par le terme «autorité de contrôle chef de file» (art. 56). La coopération entre l'autorité de contrôle chef de file et les autorités de contrôle concernées est réglée à l'art. 60. Celles-ci s'efforceront de trouver un consensus sur le projet de décision de contrôle unique préparé par l'autorité de contrôle chef de file. Le chapitre VII prévoit également une assistance mutuelle entre autorités de contrôle (art. 61) ainsi que des opérations conjointes (art. 62).

Le chapitre VIII porte sur les voies de recours, la responsabilité et les sanctions. L'art. 77 prescrit que la personne concernée a le droit d'introduire une réclamation auprès de l'autorité de contrôle. En vertu de l'art. 78, la personne concernée a également le droit de former un recours juridictionnel effectif contre une décision de l'autorité de contrôle la concernant. L'art. 80 prévoit en outre un droit pour les personnes concernées de se faire représenter à certains conditions. L'art. 83 fixe le régime général applicable aux amendes administratives que l'autorité de contrôle est habilitée à prononcer.

Le chapitre IX contient un certain nombre de dispositions réglant des situations particulières de traitement, notamment par rapport à la liberté d'expression et d'information (art. 85), à l'accès du public aux documents officiels (art. 86), aux archives, à la recherche et aux statistiques (art. 89).

4.2 Rapprochement de la législation suisse

Au sein de l'Union européenne, le règlement (UE) 2016/679 remplacera la directive 95/46/CE. N'étant pas un développement de l'acquis Schengen et Dublin, il ne liera pas la Suisse. Cela ne signifie cependant pas qu'il sera sans effets dans les domaines où elle est considérée comme un Etat tiers (domaines en dehors de la coopération Schengen et Dublin). Le règlement (UE) 2016/679 sera ainsi notamment important dans le secteur privé. En effet, comme mentionné au ch. 1.2.2.2, la Suisse bénéficie actuellement dans ce domaine d'une décision de la Commission européenne[72] constatant qu'elle garantit un niveau adéquat de protection des données. Cette décision peut néanmoins être révisée en tout temps. De plus, suite à l'arrêt Schrems, l'Union européenne a décidé d'adopter une approche plus dynamique en examinant en permanence l'évolution de la législation sur la protection des données personnelles dans les Etats tiers au bénéfice d'une décision d'adéquation. La Suisse a donc intérêt à rapprocher sa législation des exigences européennes, si elle veut rester au bénéfice de cette décision. Les critères définis à l'article 45 du règlement (UE) 2016/679 seront à l'avenir déterminants pour juger du caractère adéquat de la protection offerte par la législation suisse. Le projet devrait permettre d'assurer un niveau de protection adéquat au sens du règlement.

5 Swiss-US Privacy Shield

Les Etats-Unis n'offrent pas un niveau de protection des données personnelles suffisant. Le libre transfert de données personnelles depuis la Suisse vers cet Etat a donc nécessité l'adoption d'un cadre particulier, le «*Swiss-US Safe Harbor*»[73]. Ce régime correspondait dans une large mesure à celui en vigueur entre l'Union européenne et les Etats-Unis, le «*US-EU Safe Harbor*», validé par la Commission européenne en 2000[74]. Avec ce cadre juridique, les Etats-Unis s'engageaient à appliquer des principes offrant un niveau de protection comparable à celui de la Suisse, respectivement à celui de l'Union européenne.

Le 6 octobre 2015, la Cour de justice de l'Union européenne a invalidé la décision de la Commission européenne validant le régime de l'*US-EU Safe Harbor*[75]. Elle a estimé que la Commission européenne n'avait pas examiné que les Etats-Unis assuraient effectivement, par leur législation, leurs engagements internationaux, qu'aucune règle n'empêchait l'Etat américain d'avoir un accès illimité aux données personnelles des ressortissants de l'Union européenne et qu'il n'existait pas de moyens de protection juridique efficaces contre de telles ingérences. En février 2016, les Etats-Unis et l'Union européenne ont présenté un nouveau régime appelé

72 JO L 215 du 25.8.2000, p. 1.
73 Dans une lettre adressée le 9 décembre 2008 au Département du commerce des Etats-Unis, la Suisse a reconnu que le «*Swiss-US Safe Harbor*» offrait un niveau de protection adéquat selon l'art. 6, al. 1, LPD.
74 Décision 2000/520/CE du 26 juillet 2000.
75 Arrêt CJUE du 6 octobre 2015, aff. C-362/14, ECLI:EU:C:201 suppression de la pro650 (Schrems).

«*EU-US Privacy Shield*», qui a été adopté par la Commission européenne le 12 juillet 2016 et mis en application par les Etats-Unis le 1er août 2016.

Suite à l'arrêt de la Cour de justice de l'Union européenne précité, et au nouveau *EU-US Privacy Shield*, la Confédération (SECO), a renégocié le régime pour le transfert des données personnelles depuis la Suisse à des entreprises sises aux Etats-Unis. Le Conseil fédéral a pris acte de ce nouveau régime, appelé le «*Swiss-US Privacy Shield*» (*Privacy Shield*) le 11 janvier 2017. Le nouveau cadre correspond dans une très large mesure à la solution en vigueur entre les Etats-Unis et l'Union européenne ainsi que l'Espace économique européen (EEE).

Le *Privacy Shield* renforce les mécanismes d'application des règles par les entreprises américaines par une série de mesures. Ces dernières prévoient de nouvelles obligations pour les entreprises américaines (devoirs d'information envers les personnes concernées, devoirs de publier les décisions de la *Federal Trade Commission* [FTC] ou décision d'un tribunal, devoir de coopérer avec le Département américain du commerce [DOC] ou le préposé).

Le *Privacy Shield* renforce également les pouvoirs de gestion et de surveillance du DOC. Ainsi, par exemple, avant d'inscrire une entreprise sur la liste *Privacy Shield*, il vérifie qu'elle ait bien décrit ses activités liées à des informations obtenues de la Suisse et qu'elle précise quelles sont les informations couvertes par la certification, ainsi que la manière de rendre publique cette dernière (site Internet avec lien au site du DOC ou autre moyen). Le DOC s'engage aussi à identifier des fausses déclarations de participation au *Privacy Shield* et, à défaut de suppressions des informations erronées par l'entreprise, d'entamer des démarches juridiques et de transmettre le dossier à la FTC, au Département des transports ou à d'autres organes d'application.

Un organe arbitral a aussi été établi, pour traiter des cas de violations des principes du *Privacy Shield* par des entreprises sises aux Etats-Unis qui n'auraient pas été réparées par d'autres moyens de recours et pour lesquelles des mesures n'auraient pas – voire que partiellement – été prises. Une personne n'aura pas accès à l'organe arbitral si son cas a déjà fait l'objet d'un arbitrage contraignant ou d'un jugement, ou si sa plainte a été réglée précédemment. Les ressortissants suisses pourront déposer des plaintes auprès de cet organe et n'auront pas de frais de procédure à supporter. L'organe arbitral sera financé par des contributions des firmes américaines.

Afin de répondre aux craintes exprimées en Europe concernant en particulier l'usage abusif de données personnelles par les services de renseignements américains, le Département d'Etat a mis sur pied un *Ombudsperson*, indépendant des services de renseignements, chargé de contacter ces derniers à la demande du préposé. L'*Ombudsperson* fait directement rapport au Secrétaire d'Etat qui veillera à ce qu'il exerce sa fonction de manière objective.

Le *Swiss-US Privacy Shield* implique, pour le préposé, certaines obligations de coopération. Ce dernier transmet les plaintes des personnes concernées à la FTC, au DOC et à l'*Ombudsperson* du Département d'Etat. Du fait de la forte progression du volume d'outsourcing de traitements de données aux Etats-Unis et de l'utilisation aujourd'hui très répandue en Suisse de services de sociétés américaines telles que Facebook, Google ou Apple, on peut s'attendre à une multiplication des plaintes à traiter par le préposé. Si des entreprises certifiées se sont déclarées prêtes à colla-

borer avec lui, celui-ci doit également les soutenir dans la résolution de problèmes de protection des données. Le préposé transmet également les demandes de renseignements à l'*Ombudsperson* du Département d'Etat. Enfin, il doit désormais vérifier chaque année la qualité des mesures de protection des droits de la personnalité des personnes concernées convenues dans le *Swiss-US Privacy Shield*, en collaboration avec les offices fédéraux compétents (en autres le SECO), et établir un compte-rendu.

6 Comparaison avec des législations d'Etats non européens et n'ayant pas ratifié la convention STE 108

Afin de connaître l'état de la législation dans des pays non membres de l'Union européenne et n'ayant pas ratifié la convention STE 108, l'OFJ a donné un mandat à l'Institut Suisse de droit comparé (ISDC). L'étude[76] a principalement porté sur les points suivants: les pouvoirs et l'indépendance de l'autorité de contrôle, l'existence de bonnes pratiques, les droits des personnes concernées (par ex. voies de droit, médiation), les devoirs des responsables du traitement (par ex. devoir de documentation, analyse d'impact en matière de protection des données, existence de normes concernant les mégadonnées, le profilage, l'Internet des objets ou la portabilité des données) et enfin, la mise en œuvre de principes de protection des données dès la conception et par défaut.

Force est de constater que l'adoption d'une législation en matière de protection des données n'est plus l'apanage des Etats européens.

6.1 Argentine

L'autorité de contrôle argentine est la Direction nationale de protection des données personnelles (*Dirección Nacional de Protección de Datos Personales*, DNPDP). Ses tâches sont régies par l'art. 29 de la loi 25.326[77]. Elle a un rôle d'assistance, de conseil et de surveillance. L'art. 29 du décret 1558/2001[78] lui permet également d'établir des règles administratives et de procédure par rapport au registre des bases de données personnelles (*Registro*), qui permet d'identifier et de contrôler les bases de données personnelles. Ce même art. 29 prévoit que la DNDPD peut traiter les plaintes et les réclamations déposées aux termes de la loi 25.326. La DNDPD est aussi tenue d'approuver les codes de conduite adoptées par les entités représentatives des usagers ou responsables de bases de données (art. 30 de la loi 25.326).

76 Ces informations se basent sur un avis de droit de l'ISDC du 3 août 2016.
77 Ley 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables archivios, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: Octubre 4 de 2000, disponible sous www.jus.gob.ar/media/33481/ ley_25326.pdf.
78 Decreto 1558/2001, Protección de los datos personales, disponible sous www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

L'art. 14 de la loi 25.326 institue un droit d'accès, qui donne aux personnes concernées le droit d'obtenir des informations sur leurs données personnelles détenues dans des bases de données privées ou publiques. Lorsque la demande est déposée, un délai de dix jours est octroyé au responsable pour y répondre. Passé ce délai, les personnes intéressées peuvent agir par la voie d'un recours. L'art. 16 permet aux personnes physiques de demander la rectification, l'actualisation ou l'effacement de données les concernant. Le responsable de la base de données a un délai de cinq jours pour répondre à la demande. Il ne peut la refuser qu'en cas de nécessité pour la protection de l'Etat, de l'ordre public, de la sécurité publique ou pour les intérêts de tiers. Passé le délai de cinq jours, ou en cas de réponse négative, la personne intéressée peut interjeter un recours.

Les responsables du traitement ont comme principales tâches d'inscrire les bases de données dans le *Registro*, de veiller à la sécurité des données stockées, de garantir la confidentialité des données ainsi que de fournir les documents et renseignements sollicités par la DNPDP.

La législation sur la protection des données s'applique aussi aux mégadonnées dans les cas où, de l'ensemble des données collectées, il est possible d'identifier une personne en particulier. En ce qui concerne le profilage, l'art. 27 du Décret 1558/2001 contient une règle sur le profilage dans le domaine de la publicité. Selon cet article, il est possible de collecter, traiter et transmettre des données sans le consentement de la personne lorsque le but est de créer des profils afin de catégoriser des préférences et des comportements. Cette possibilité est soumise à deux conditions: les personnes concernées ne doivent être identifiées que par leur appartenance à un groupe générique, et l'étendue des données individuelles collectées doit être limitée au strict nécessaire. En outre, dans toute communication à but publicitaire, la possibilité pour le titulaire des données de demander leur retrait ou leur blocage doit être mentionnée.

Enfin, ce qui concerne la mise en œuvre du principe de protection des données dès la conception et par défaut, le DNPDP a approuvé un guide de bonnes pratiques dans le développement d'applications informatiques, qui s'adresse aux développeurs d'applications. Il a surtout pour but de rappeler le devoir des développeurs de veiller au respect de la vie privée des personnes et ceci dès le début de la création de l'application.

6.2 Nouvelle-Zélande

En Nouvelle-Zélande, la protection des données est principalement régie par le *Privacy Act 1993*[79]. Un processus de révision est en cours et le projet d'un nouveau *Privacy Act* devrait être mis en consultation avant la fin de l'année 2016, avec pour but d'être présenté au Parlement en 2017.

La réforme prévue touche principalement les fonctions de l'autorité publique chargée de la surveillance de la protection des données, appelée *Privacy Commissionner*

79 Le «*Privacy Act* 1993» est disponible sous: www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

(PC). Le PC, qui est déjà maintenant tenu d'approuver les codes de bonnes pratiques, verra son rôle se renforcer. Un système de déclaration obligatoire des violations de données sera en effet introduit et sera accompagné par deux améliorations pour le PC: il pourra dorénavant faire des requêtes urgentes afin d'obtenir des informations qu'il juge nécessaires et il sera en mesure d'émettre des avis de conformité pour les violations du *Privacy Act*.

La réforme n'a pas pour but de renforcer les droits des particuliers, car ils sont considérés comme étant suffisants dans le *Privacy Act* 1993. Sa partie 2, *Information Privacy Principles* (IPP) octroie en effet aux individus des droits. En particulier, l'IPP 6 permet aux personnes concernées de demander si des données les concernant sont détenues et d'y avoir accès. L'IPP 7 permet aux personnes concernées de demander des rectifications aux données les concernant et, si la demande est rejetée, qu'une déclaration soit attachée aux données montrant qu'une demande de modification a été sollicitée.

Actuellement, toutes les agences[80] doivent s'assurer qu'il y ait au moins un *Privacy Officer* (PO) au sein de l'agence. Les devoirs des PO sont d'encourager la conformité aux différents IPP, de s'occuper des requêtes faites auprès de l'agence et de collaborer avec le PC pour les enquêtes concernant l'agence. La réforme occasionnera deux importants changements dans les devoirs des agences: elles auront le devoir d'annoncer au PC certaines violations de la protection des données et un nouvel IPP demande aux agences de prendre les mesures raisonnables pour avoir une protection des données acceptable lors d'échanges avec des pays étrangers.

Le PC a un rôle important pour la mise en œuvre du principe de protection des données dès la conception et par défaut. En effet, la section 13, ch. (1), let. (n), du *Privacy Act 1993* lui donne l'opportunité d'entreprendre des recherches et de suivre l'évolution du traitement des données et des nouvelles technologies liées à l'informatique, et surtout de veiller à ce que les effets négatifs de ces développements sur le niveau de protection de la vie privée des individus soient minimisés. Par ce biais, le PC peut promouvoir le *privacy by design*. La réforme ne prévoit pas d'autres règles en ce qui concerne le *privacy by design* et *by default*.

6.3 Corée du Sud

La Corée du Sud a une législation dans le domaine de la protection des données depuis 2011, le *Personal Information Protection Act* (PIPA).

De par son histoire et ses nombreuses lois, la Corée du Sud a un système assez complexe, ce qui se traduit par plusieurs autorités liées à la protection des données. Pour les questions de régulation, la responsabilité revient à la *Personal Information Protection Commission*. Pour la médiation lors de plaintes individuelles ou collectives, c'est le *Personal Information Dispute Mediation Committee* qui s'en charge. Ce comité peut proposer, lors de divergences entre les personnes concernées et des institutions traitant des données, une proposition de conciliation (art. 47 PIPA). Les

80 Sont considérées comme «*agency*» presque toutes les personnes et organisations qui détiennent des données personnelles.

plaintes liées aux technologies de l'information sont traitées par la *Korea Internet & Security Agency*, qui possède une hotline et a également développé un certain nombre de guides et de recommandations pour le secteur privé. Quant au Ministère de l'intérieur, il tient un rôle important dans la mise en œuvre de la législation sur la protection des données. Il est compétent pour concevoir un *Data Protection Basic Plan*, valable trois ans (art. 9 PIPA), ainsi que des lignes directrices (art. 12 PIPA).

Selon l'art. 4 PIPA, les particuliers ont le droit de s'informer sur le traitement des données les concernant. Ils ont le droit par ce biais de demander la suppression ou la rectification de certaines données. La loi prévoit également un droit à des dommages-intérêts.

Lors du traitement de données, le responsable du traitement doit obtenir le consentement de la personne concernée (art. 22 PIPA). Il a aussi l'obligation d'informer cette dernière lorsqu'il traite des données reçues d'une tierce personne (art. 20 PIPA). Enfin, il doit détruire les données après le délai convenu ou après avoir atteint son but (art. 21 PIPA). Le chapitre IV PIPA institue également des garanties que le responsable du traitement doit assurer. En particulier, l'art. 29 oblige les responsables à prendre toutes les mesures spécifiques physiques, techniques et administratives pour prévenir la perte, le vol, la diffusion, la falsification ou la destruction de données. L'information doit être traitée d'une manière qui minimise les risques de violations de la vie privée (art. 3, par. 6, PIPA) et en anonymisant autant que possible les données (art. 3, par. 7, PIPA).

En outre, le responsable du traitement dans une entreprise doit adopter et publier une stratégie de protection des données (*privacy policy*) (art. 30 PIPA). Il est également demandé à ce qu'un conseiller à la protection des données soit désigné (*privacy officer*) (art. 31 PIPA). De leur côté, les institutions publiques doivent enregistrer leurs collectes de données (art. 32 PIPA) et effectuer une étude d'impact du traitement (art. 35 PIPA), qui est également enregistrée.

6.4 Japon

Le Japon est doté depuis 2016 d'une autorité de contrôle en matière de protection des données (*Personal Information Protection Commission*) qui exerce des fonctions de surveillance, de régulation et de médiation. Deux autres institutions méritent d'être mentionnées. Au niveau du secteur privé, la loi sur la protection des données adoptée en 2003 (*Act on the Protection of Personal Information* [APPI][81]) permet à des organisations privées de protection des données ayant reçu une accréditation ministérielle de traiter des recours dirigés contre des entreprises et de délivrer des informations aidant à une meilleure application de la protection des données; elles ont en outre la possibilité de prendre les mesures nécessaires à la mise en œuvre des principes relatifs à la protection des données (art. 37 APPI). En ce qui concerne le secteur public, l'*Information Disclosure and Personal Information Protection*

81 L'APPI est disponible en anglais à l'adresse suivante: www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

Review Board est l'autorité compétente pour garantir la protection des données dans les enquêtes en matière de transparence.

L'APPI donne le droit aux particuliers d'obtenir des informations sur l'existence et le but d'un traitement de données (art. 24, al. 2, et 25 APPI). Des émoluments peuvent être perçus pour le traitement de la requête (art. 30 APPI). En outre, les personnes concernées peuvent exiger la rectification, le complément ou la suppression de données erronées. A ce titre, le responsable du traitement a le devoir d'examiner les griefs avancés et d'informer la personne concernée en cas de rejet de sa requête (art. 30 APPI). Les particuliers peuvent également obtenir la suspension d'un traitement de données ou leur suppression lorsqu'un tel traitement contredit son but ou lorsque les données ont été obtenues par des moyens illicites. Une telle requête n'est cependant pas admissible lorsqu'elle est susceptible d'engendrer des coûts élevés ou lorsqu'elle s'avère trop compliquée et que le responsable du traitement a pris d'autres mesures pour protéger les données et les intérêts de la personne concernée (art. 27 APPI). Les mêmes principes s'appliquent au transfert de données à des tiers (art. 27, al. 2, APPI).

Le responsable du traitement doit spécifier le but du traitement de la manière la plus précise possible (art. 15, let. f, APPI). En outre, les informations concernant le but du traitement et les droits des personnes concernées doivent être mises à la disposition du public (art. 24 APPI). Le responsable du traitement doit également obtenir l'accord des personnes concernées, bien qu'un accord tacite semble suffire. Il ne peut obtenir des données par le biais de moyens trompeurs ou illicites (art. 17 APPI) et doit s'efforcer de maintenir l'exactitude des données. Le transfert des données à des tiers n'est possible que dans certains cas particuliers (par ex. en vue de protéger la vie ou l'intégrité physique de quelqu'un, de protéger la santé publique ou dans le cadre de la collaboration avec les autorités; art. 23 APPI). D'une manière générale, des mesures de sécurité visant à éviter la perte ou l'endommagement de données doivent être prises (art. 20 APPI) et les personnes chargées du traitement des données doivent faire l'objet d'une surveillance (art. 21, let. f, APPI). La loi ne prévoit en revanche aucun devoir d'information en cas de perte de données.

Outre l'art. 20 APPI déjà mentionné, il n'existe pas d'information relative à des mesures spécifiques visant à promouvoir le principe de protection des données dès la conception et par défaut. On peut cependant s'attendre à ce que l'autorité de surveillance prenne prochainement des mesures en ce sens.

6.5 Singapour

L'autorité de contrôle est la *Personal data protection commission* (PDPC), créée en 2013 afin de mettre en œuvre le *Personal Data Protection Act* (PDPA)[82], entré en vigueur en 2012. La PDPC exerce, entre autres, une fonction de surveillance et de régulation sur les traitements de données effectués par des organismes privés (le

82 Le PDPA est disponible en anglais à l'adresse suivante: statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Satuts%3Ainforce;rec=0.

PDPA n'est pas applicable au secteur public). Elle peut à cet égard édicter des directives ou rendre des décisions pour assurer le respect du PDPA et même prononcer une amende d'un montant maximal de 1 million de dollars en cas de non-respect de la loi (art. 28 et 29 PDPA). La PDPC dispose à cet égard d'importants moyens d'investigation, allant du droit de pénétrer sur des biens-fonds privés au droit d'exiger la délivrance d'informations et de documents qui peuvent être mis sous séquestre (annexe 9 PDPA). Cependant, la PDPC peut également tenter de résoudre les litiges par la voie d'une médiation (art. 27 PDPA). En outre, la PDPC élabore et met en œuvre des politiques publiques (par ex. par l'adoption de lignes de conduite) afin de sensibiliser les différentes organisations et les particuliers au respect de la protection des données. Enfin, la PDPC représente le gouvernement singapourien au niveau international pour toutes les questions liées à la protection des données (art. 6 PDPA).

Les personnes concernées peuvent requérir l'accès à leurs données personnelles détenues ou contrôlées par une organisation. Ils ont également le droit d'obtenir des informations sur la façon dont leurs données personnelles ont été utilisées ou communiquées dans l'année précédant leur demande, à moins qu'un intérêt public ou privé prépondérant ne s'y oppose (art. 21 PDPA). Les personnes concernées peuvent en outre exiger la correction d'une erreur ou d'une omission dans leurs données personnelles (art. 22 PDPA).

Les responsables du traitement sont en principe tenus de s'assurer du consentement exprès ou tacite des personnes concernées dès qu'ils collectent, utilisent ou communiquent des données personnelles. L'exigence du consentement de la personne concernée est cependant moins forte que dans les autres ordres juridiques étudiés. En effet, le droit singapourien prévoit de nombreuses exceptions en vertu desquelles le consentement n'est pas nécessaire ou peut être présumé (art. 13 à 15 PDPA). Le traitement des données doit être effectué dans un but connu de la personne concernée ou dans un but qui semblerait raisonnable à tout individu placé dans les mêmes circonstances (art. 18 PDPA). Les responsables du traitement doivent s'efforcer de maintenir l'exactitude des données (art. 23 PDPA) et sont tenus de prendre les mesures de précaution propres à éviter la fuite, la copie ou un accès non autorisé aux données personnelles en leur possession (art. 24 PDPA). Les responsables du traitement doivent détruire ou rendre anonymes les données personnelles dès lors que leur conservation ne correspond plus au but de leur collecte et qu'aucun motif juridique ou économique ne permet de justifier leur maintien (art. 25 PDPA). Enfin, la communication transfrontière de données personnelles n'est autorisée qu'à la condition que le pays destinataire garantisse un niveau de protection équivalent à celui de Singapour (art. 26 PDPA).

Aucune action visant spécifiquement à promouvoir le principe de protection des données dès la conception et par défaut ne semble avoir été prise. Cela étant, le pouvoir de mener des actions de sensibilisation à la protection des données que la loi octroie à la PDPC (art. 6 PDPA) pourrait lui permettre d'entreprendre la promotion de ce principe.

7 Mise en œuvre

Dans le cadre de l'AIR, il a été demandé que l'on évite autant que possible d'utiliser des notions juridiques indéterminées. La LPD est une loi-cadre qui n'est pas liée à une technologie particulière, qui doit rester applicable aux situations les plus variées et qui doit pouvoir évoluer. Les codes de conduite permettent de préciser certaines notions ainsi que les modalités de certains droits et devoirs, en tenant compte des caractéristiques des différents domaines. En outre, le préposé pourra continuer à élaborer des guides et des outils pour soutenir les responsables du traitement et les sous-traitants dans l'accomplissement de leurs tâches et les personnes concernées dans l'exercice de leurs droits.

Au demeurant, l'ordonnance du 14 juin 1993 sur la protection des données (OLPD)[83] sera adaptée afin de ne pas surcharger la loi de détails.

Si le projet ne prévoit pas expressément une évaluation de sa mise en œuvre, l'efficacité de ses mesures sera évaluée conformément à l'art. 170 Cst. De plus, comme c'est le cas aujourd'hui, le préposé doit établir régulièrement un rapport d'activité à l'intention de l'Assemblée fédérale. Les informations contenues dans ce rapport permettent d'avoir une vue d'ensemble de la mise en œuvre de la future LPD.

Enfin, dans la mesure où la reprise par la Suisse de la directive (UE) 2016/680 et la ratification par celle-ci du protocole d'amendement de la convention STE 108 lient également les cantons, ceux-ci doivent adapter leurs législations cantonales dans la mesure où elles ne remplissent pas les exigences de ces instruments.

8 Classement des interventions parlementaires

Les interventions parlementaires suivantes peuvent être classées:

- Postulat Hodgers 10.3383 «Adapter la loi sur la protection des données aux nouvelles technologies». En révisant la LPD pour l'adapter aux nouvelles technologies, le Conseil fédéral a réalisé le postulat.
- Postulat Graber 10.3651 «Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles». Ce postulat a partiellement été réalisé dans le cadre du rapport d'évaluation de la LPD. Avec le projet de révision, le Conseil fédéral donne suite aux questions restantes, à savoir sur les limites qu'il entend assigner aux technologies de surveillance et de collecte de renseignements et sur la question de savoir s'il juge opportun de proposer un renforcement de la législation protectrice de la sphère privée et des données personnelles.
- Postulat Schwaab 12.3152 «Droit à l'oubli numérique». Le Conseil fédéral a étudié l'opportunité de régler ou de préciser dans la législation un droit à «l'oubli numérique» et les modalités pour en faciliter l'usage par les consommateurs. Le droit à l'oubli, numérique ou non, existe déjà dans la LPD. En mentionnant expressément le «droit à l'effacement» dans le P-LPD, le

83 RS **235.11**

Conseil fédéral entend faciliter la lecture de la loi pour les personnes concernées. Des dispositions plus détaillées sur des questions numériques contreviendraient au caractère technologiquement neutre de la loi. Le Conseil fédéral préconise de recourir pour ce domaine aux codes de conduite des milieux concernés et aux guides du préposé.

– Postulat Recordon 13.3989 «Violations de la personnalité dues au progrès des techniques de l'information et de la communication». Dans le cadre des travaux de révision, le Conseil fédéral a examiné les nouvelles menaces que représentent les nouvelles technologies pour les droits de la personnalité. Le P-LPD prévoit des mesures pour améliorer la protection de ces derniers.

– Motion Comte 14.3288 «Faire de l'usurpation d'identité une infraction pénale en tant que telle». La motion a été réalisée par l'introduction, dans le P-CP, de l'art. 179^{decies}.

– Postulat Derder 14.3655 «Définir notre identité numérique et identifier les solutions pour la protéger». Le Conseil fédéral a examiné l'opportunité de définir l'identité numérique dans le cadre du projet. Il y a renoncé, vu le caractère technologiquement neutre de la loi. Les mesures proposées permettent cependant aussi de mieux protéger les personnalités numériques des citoyens. Par ailleurs, la question de l'identité numérique sera approfondie par le groupe d'experts «Avenir du traitement et de la sécurité des données», dont les travaux se termineront en 2018.

– Postulat Schwaab 14.3739 «Control by design. Renforcer les droits de propriété pour empêcher les connexions indésirables». Le P-LPD réalise le postulat en ce sens que son contenu protège mieux à l'avenir les personnes concernées. Les autres aspects du postulat, à savoir essentiellement des questions liées à la sécurité des produits et de l'Internet, seront approfondis par le groupe d'experts «Avenir du traitement et de la sécurité des données».

– Postulats Groupe libéral-radical 14.4137 et Comte 14.4284 «Enregistrements vidéo par des privés. Mieux protéger la sphère privée». Le P-LPD prévoit de renforcer le volet pénal de la loi. Dorénavant, la collecte de données en violation du devoir d'informer – devoir qui a été étendu dans le secteur privé à tous les types de données – peut être sanctionnée plus efficacement. Associée aux dispositions pénales actuelles sur les infractions contre le domaine secret ou le domaine privé, cette modification offre une protection élargie. Le projet prévoit d'ailleurs expressément qu'un risque élevé pour la personnalité et les droits fondamentaux de la personne concernée justifiant la réalisation d'une analyse d'impact en matière de protection des données personnelles, est, entre autres, réalisé lorsque le domaine public est systématiquement surveillé sur une grande étendue.

– Postulat Béglé 16.3383 «Données numériques. Informer les personnes lésées en cas de piratage». Le P-LPD (art. 22) prévoit une annonce des violations de la sécurité des données au préposé et, dans certaines situations, l'information de la personne concernée. Le contenu de l'information sera précisé dans l'ordonnance.

– Postulat Béglé 16.3384 «Données numériques médicales. Assurer une collecte protégée, transparente et ciblée dans la révision de la loi sur la protection des données». La LPD s'applique aux données médicales dans les limites des lois spéciales. Le P-LPD prévoit toute une série de nouvelles obligations à charge du responsable du traitement et du sous-traitant, qui pourront ainsi selon les cas aussi valoir pour les données médicales. Ces obligations vont dans le sens du postulat. D'autres mesures, telles que le renforcement des pouvoirs du préposé et des sanctions pénales ou l'élaboration de codes de conduite et de guides, devraient aussi permettre d'améliorer la protection des données médicales.

Les interventions parlementaires suivantes sont réalisées partiellement:

– Postulat Schwaab 14.3782 «Des règles pour la «mort numérique». L'art. 16 P-LPD prévoit d'une part un droit de consulter les données d'une personne décédée et, d'autre part, la possibilité pour les héritiers et l'éventuel exécuteur testamentaire, d'exiger l'effacement de données d'une personne décédée. Les points principaux du postulat sont ainsi mis en œuvre. Les autres aspects seront étudiés dans le cadre de la révision du droit des successions.

– Postulat Derder 15.4045 «Droit d'exploiter des données personnelles. Droit d'obtenir une copie». Le Conseil fédéral estime que l'introduction d'un droit à la portabilité sur les données n'est pas souhaitable dans le cadre de la révision de la LPD (cf. ch. 1.7.4). Cette question sera examinée dans le cadre de la Stratégie «Suisse numérique» (cf. ch. 1.1.3).

– Postulat Béglé 16.3386 «Réappropriation des données personnelles. Favoriser l'autodétermination informationnelle». Le P-LPD ne prévoit pas de concrétiser le droit de se réapproprier ses données personnelles, pour les mêmes raisons que pour la portabilité des données (1.7.4). Cette question sera examinée dans le cadre de la Stratégie «Suisse numérique» (cf. ch. 1.1.3).

– Postulat Schwaab 16.3682 «Encadrement des pratiques des sociétés de renseignements de solvabilité». S'agissant d'une réglementation générale, le P-LPD n'introduit pas de dispositions visant à régler spécifiquement les activités des sociétés de renseignements de solvabilité. Néanmoins, la protection des personnes concernées est améliorée puisque le P-LPD renforce la transparence des traitements, les droits de ces personnes, les obligations du responsable du traitement et la surveillance par le préposé. De plus, le P-LPD restreint les conditions du motif justificatif permettant à un responsable du traitement de traiter des données personnelles dans le but d'évaluer la solvabilité de la personne concernée (art. 27, al. 2, let. c, P-LPD). Dans le cadre du rapport donnant suite au postulat susmentionné, le Conseil fédéral entend examiner l'opportunité d'adopter une législation spécifique régissant les activités des sociétés de renseignements de solvabilité et les solutions légales envisageables.

9 Commentaire des dispositions

9.1 P-LPD

9.1.1 Préambule

Le Conseil fédéral considère qu'il est opportun d'introduire dans le préambule l'art. 97, al. 1, Cst., qui donne à la Confédération la compétence de légiférer sur la protection des consommateurs. En effet, le P-LPD consacre un certain nombre de dispositions qui renforcent notamment la transparence des traitements de données personnelles, le contrôle par les personnes concernées et le système de surveillance par le préposé. Les consommateurs sont ainsi mieux protégés.

9.1.2 But, champ d'application et autorité fédérale de surveillance

Art. 1 But

Le but de la future LPD est identique à celui du droit en vigueur (art. 1 LPD). La LPD concrétise au plan légal le droit à l'autodétermination en matière informationnelle de l'art. 13, al. 2, Cst., à savoir le droit pour la personne concernée de pouvoir déterminer elle-même si et dans quels buts des informations à son sujet peuvent être traitées[84].

L'art. 1 subit une modification rédactionnelle: la protection est dorénavant expressément limitée aux personnes physiques. Cette adaptation est rendue nécessaire par la modification du champ d'application de la loi (cf. commentaire de l'art. 2 P-LPD).

Art. 2 Champ d'application

Le champ d'application de la loi est élargi afin de tenir compte notamment des exigences du P-STE 108. Il est prévu de modifier l'exception concernant les procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif (art. 2, al. 2, let. c, LPD), et celle concernant les registres publics relatifs aux rapports juridiques de droit privé (art. 2, al. 2, let. d).

Pour le reste, le P-LPD reste, à l'instar de la LPD, une législation générale sur la protection des données. Par conséquent, si des traitements de données personnelles sont régis par des dispositions de protection des données prévues dans d'autres lois fédérales, celles-ci sont en principe applicables en vertu du principe de la priorité des dispositions spéciales sur les dispositions générales[85].

Al. 1 Application aux personnes physiques

La future LPD s'applique au traitement de données personnelles concernant des personnes physiques par des personnes privées et des organes fédéraux.

84 ATF **140** I 2, consid. 9.1.
85 Cf. ATF **128** II 311, consid. 8, FF **1988** 421, 452 et Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, N 286 ss.

Suppression de la protection des personnes morales

Le P-LPD renonce à prévoir une protection des données personnelles des personnes morales; les textes de protection des données de l'Union européenne et du Conseil de l'Europe ainsi que la majorité des législations étrangères ne prévoient pas une telle protection. Cette dernière a d'ailleurs peu de portée pratique et le préposé n'a à ce jour jamais émis de recommandations en la matière. Par ailleurs, la large protection conférée par les art. 28 ss du code civil (CC)[86] (atteintes à la personnalité, par ex. à la réputation), par la LCD, par la loi fédérale du 9 octobre 1992 sur le droit d'auteur[87], par les règles sur les secrets professionnels, d'affaires et de fabrication, ou, au plan constitutionnel, par l'art. 13 Cst., reste inchangée. La modification prévue permet en revanche d'améliorer la loi là où elle souffre actuellement d'un défaut de mise en œuvre, et de lui assurer une meilleure crédibilité[88]. Cette solution a aussi pour avantage de ne plus soumettre la communication à l'étranger de données concernant des personnes morales à la condition qu'un niveau de protection adéquat soit garanti dans l'Etat de destination (art. 13 P-LPD), ce qui devrait favoriser les flux transfrontières. Il est également important de noter que la majorité des experts consultés dans le cadre de l'AIR et des participants à la consultation externe s'est montrée favorable à la suppression de la protection des données personnelles des personnes morales[89]. Enfin, il en va de même du Parlement, qui a refusé de donner suite à une motion qui demandait que la protection des personnes morales soit maintenue[90].

Dans le domaine du traitement des données par des organes fédéraux, la suppression de la protection des données des personnes morales a pour conséquence que les bases légales qui autorisaient les organes fédéraux à traiter des données ne sont plus applicables lorsqu'il s'agit de données concernant des personnes morales. Selon l'art. 5 Cst. le droit est la base et la limite de l'activité de l'Etat. Le projet de loi prévoit ainsi une série de dispositions dans la LOGA, qui règlent la question du traitement des données concernant des personnes morales par les organes fédéraux (cf. ch. 9.2.8). En outre, une disposition transitoire empêche d'éventuelles lacunes juridiques pendant cinq ans (cf. art. 66 P-LPD et les explications au ch. 9.1.11)

La loi du 17 décembre 2004 sur la transparence (LTrans)[91] confère à toute personne le droit de consulter les documents officiels des autorités fédérales qui sont assujetties au principe de transparence. Le nouveau champ d'application du P-LPD a pour conséquence que le droit d'accès à des documents contenant des données de personnes morales ne pourra plus être restreint pour des motifs de protection des données mais uniquement si l'accès risque de révéler des secrets professionnels, d'affaires ou de fabrication (art. 7, al. 1, let. g, LTrans) ou s'il existe un risque d'atteinte à la sphère privée de celle-ci, par exemple à sa réputation (art. 7, al. 2, LTrans). Afin de garantir la protection des droits des personnes morales lorsqu'une

86 RS **210**
87 RS **231.1**
88 Sur cette question, cf. Drechsler Christian, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, PJA 2016, pp. 80 ss et 85–86.
89 Voir la AIR, p. 46.
90 Motion Béglé 16.3379 «Promouvoir la Suisse en tant que coffre-fort numérique universel.»
91 RS **152.3**

demande d'accès porte sur des documents contenant des informations qui pourraient, en cas de divulgation, porter atteinte à leur sphère privée, le projet de loi modifie certaines dispositions de la LTrans (ch. 9.2.6).

L'abrogation de la protection des personnes morales a également pour conséquence que celles-ci ne peuvent plus faire valoir un droit d'accès en vertu du P-LPD mais peuvent faire valoir leurs droits de procédure et, le cas échéant, invoquer la LTrans pour consulter des documents officiels contenant des informations les concernant.

Al. 2 Exceptions au champ d'application

L'al. 2 P-LPD maintient l'exception au champ d'application de la loi concernant les traitements de données effectués par une personne physique pour un usage exclusivement personnel (*let. a*); la modification rédactionnelle n'implique aucun changement.

Les traitements de données effectués par les Chambres fédérales et les commissions parlementaires dans le cadre de leurs délibérations restent également exclus du champ d'application de la loi, pour les mêmes motifs que ceux invoqués par le Conseil fédéral dans son message du 23 mars 1988[92] (*let. b*).

Conformément à la *let. c,* les bénéficiaires institutionnels selon l'art. 2, al. 1, de la loi du 22 juin 2007 sur l'Etat hôte (LEH)[93] qui jouissent en Suisse d'une immunité de juridiction, ne sont pas soumis à la LPD. Il s'agit ainsi de maintenir la situation actuelle s'agissant du CICR et de mentionner explicitement les autres bénéficiaires institutionnels concernés. Ces derniers jouissent en effet eux aussi, en vertu du droit international et de la LEH, de l'indépendance et de la liberté d'action qui leur sont nécessaires pour accomplir leurs fonctions internationales. On ne saurait attendre d'un Etat qu'il se plie aux règles du droit suisse pour les données traitées par ses représentations diplomatiques ou consulaires en Suisse, de même que la Suisse ne doit pas suivre les prescriptions y relatives étrangères pour son réseau de représentations à l'étranger. On ne saurait pas non plus imposer à une organisation internationale qui a, par définition, des activités dans de nombreux Etats, de suivre les exigences du droit national de chacun des Etats dans lesquels elle est active; cela la mettrait dans l'incapacité de mener ses activités statutaires.

Al. 3 Traitement de données personnelles dans le cadre d'une procédure

Aux termes de l'art. 2, al. 3, P-LPD, les traitements de données personnelles effectués dans le cadre de procédures devant des tribunaux ou dans le cadre de procédures régies par les dispositions de la procédure fédérale, ainsi que les droits des personnes concernées, obéissent au droit de procédure applicable. La norme règle le rapport entre la LPD et le droit de procédure, et fixe comme principe général que seul le droit de procédure applicable détermine d'une part la manière dont les données personnelles sont traitées dans les procédures et d'autre part les droits des personnes concernées. Le droit de procédure garantit également la protection de la personnalité et des droits fondamentaux de toutes les personnes impliquées, offrant ainsi une protection équivalente à celle de la LPD. Si la LPD s'appliquait dans ce

92 FF **1988** II 449
93 RS **192.12**

domaine, on serait confronté à un risque de conflits de normes et de contradictions, qui pourrait perturber le la bonne application des règles de procédure. C'est la raison pour laquelle l'art. 9, ch. 1, let. a, P-STE 108 prévoit une exception du même type. Sur le fond, la règle du P-LPD correspond au droit en vigueur.

L'exception prévue à l'al. 3 concerne d'abord les «procédures devant des tribunaux», ce qui inclut toutes les procédures devant les tribunaux pénaux, civils et administratifs cantonaux et fédéraux, mais aussi devant les tribunaux arbitraux ayant leur siège en Suisse. Elle concerne aussi toutes les procédures régies par les dispositions de la procédure fédérale, quelle que soit l'autorité devant laquelle elles se déroulent. Font notamment partie des dispositions de la procédure fédérale la loi du 17 juin 2005 sur le Tribunal fédéral (LTF)[94], la loi du 17 juin 2005 sur le Tribunal administratif fédéral (LTAF)[95], la loi du 20 mars 2009 sur le Tribunal fédéral des brevets (LTFB)[96], la PA à l'exception des procédures administratives de première instance, le code de procédure civile (CPC)[97], la loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP)[98], le CPP, la DPA, la procédure pénale militaire du 23 mars 1979[99] et l'EIMP.

Contrairement au droit en vigueur, le P-LPD abandonne la notion de «procédure pendante», car il n'est question de litispendance que dans la procédure civile, et que ce terme a, de ce fait, causé parfois des problèmes de délimitation. Ce qui compte à présent, c'est de savoir si une procédure a lieu devant un tribunal ou si elle est régie par les dispositions de la procédure fédérale. Une procédure a lieu devant un tribunal lorsque celui-ci est saisi d'une affaire pour la première fois et que la procédure a été engagée conformément au droit de procédure applicable. Elle est régie par les dispositions de la procédure fédérale dès lors qu'un état de fait particulier est traité par une autorité conformément aux prescriptions de l'une de ces lois. Le droit de procédure reste applicable, y compris après la clôture de la procédure. Pour éviter que le dossier puisse être modifié après-coup par des instruments étrangers à la procédure, le droit de procédure prévoit des procédures autonomes pour le suivi, la consultation et la conservation des dossiers. En résumé, le critère de délimitation majeur pour la non-applicabilité de la LPD est l'existence ou non, au point de vue fonctionnel, d'un lien immédiat avec une procédure (devant un tribunal). Un tel lien existe lorsque le traitement de données personnelles en question est susceptible d'avoir des effets concrets sur cette procédure ou sur son issue, ou sur les droits procéduraux des parties.

Dès lors que la prescription de l'al. 3 vient à s'appliquer, seul le droit de procédure applicable régit le traitement des données personnelles et les droits des personnes concernées, qu'il s'agisse du traitement de données effectué par le tribunal vis-à-vis des parties à la procédure ou de celui effectué par les parties vis-à-vis d'autres parties. Cela vaut en particulier pour les droits des parties de prendre connaissance des données intégrées à la procédure et d'en rectifier certaines si nécessaire, de

94 RS **173.110**
95 RS **173.32**
96 RS **173.41**
97 RS **272**
98 RS **281.1**
99 RS **322.1**

même que pour le traitement de données dans les procédures judiciaires en général. Cela signifie notamment que les différents moyens de recours prévus par la LPD ne s'appliquent ni au traitement de données effectué par le tribunal dans la procédure, ni à celui effectué par les autres parties. A titre d'exemple, les parties ne peuvent pas faire valoir de droit d'accès au sens de la LPD afin de consulter le dossier au tribunal ou de fournir des preuves à d'autres parties (cf. ch. 9.1.5). En d'autres termes, il n'est pas possible de s'appuyer sur la LPD pour entreprendre vis-à-vis du tribunal ou des autres parties des actions relevant de la procédure qui seraient soit exclues selon le droit de procédure en question, soit régies par des règles et des principes bien précis. Le droit de procédure continue de régir exclusivement la modification des dossiers (rectification, commentaire, révision) à l'issue de la procédure, car les dossiers doivent être conformes au résultat d'une procédure. Ce faisant il n'est pas exclu que le droit de procédure pertinent déclare que la LPD est applicable après la clôture de la procédure (cf. art. 99 CPP). Si le droit applicable ne prévoit rien s'agissant du droit pour des tiers de consulter le dossier après la clôture de la procédure, il convient, pour déterminer le régime applicable, de s'orienter d'après les dispositions de la LPD.

Contrairement à ce que prévoyait encore le projet mis en consultation, l'al. 3 n'exclut donc plus uniquement du champ d'application de la LPD les traitements de données effectués par certaines institutions, ce qui avait été vivement critiqué lors de la consultation. Il en exclut aussi les traitements de données effectués par les parties. Il règle par ailleurs le conflit de normes d'une manière différente, en ce sens que c'est la norme qui détermine le droit applicable. Quoi qu'il en soit, les tribunaux fédéraux, en particulier, restent exclus du champ d'application de la LPD en ce qui concerne les traitements de données effectués dans le cadre de leur activité juridictionnelle. La séparation des pouvoirs est donc respectée.

Il découle aussi de l'art. 2, al. 3, que la LPD est applicable aux traitements de données effectués par les services administratifs de tribunaux et d'autorités, notamment de données relatives au personnel[100]. Les tribunaux sont aussi tenus de respecter les prescriptions de la LPD relatives à la sécurité des données pour l'archivage des preuves et des arrêts. Il existe toutefois des dérogations à la surveillance exercée par le préposé (cf. art. 3, al. 2, P-LPD et son commentaire).

La prescription de l'art. 2, al. 3, P-LPD ne s'applique pas, conformément à la 2e phrase, aux procédures administratives de première instance. Cette règle du droit en vigueur est maintenue telle quelle.

Al. 4 Registres publics relatifs aux rapports de droit privé

L'exception concernant les registres publics relatifs aux rapports de droit privé, telle qu'elle est prévue à l'art. 2, al. 2, let. d, LPD, n'est pas compatible avec les exigences de l'art. 3 P-STE 108. En effet, la future convention ne prévoit pas d'exception pour ce type de registres. Il en va de même du règlement (UE) 2016/679.

Si les personnes concernées ont un intérêt à ce que les registres publics relatifs aux rapports de droit privé respectent les principes de protection des données personnelles, il existe également un intérêt public à la tenue de ces registres et à leur accès

100 Cf. FF **1988** II 450

(cf. consid. 73 du règlement (UE) 2016/679). Dans un arrêt du 9 mars 2017[101], la Cour de justice de l'Union européenne a eu l'occasion de se prononcer sur l'articulation entre la protection des données et la publicité d'un registre des sociétés tenu par les autorités italiennes. Dans cette affaire, un ancien administrateur et liquidateur d'une société mise en faillite exigeait la radiation de certaines données personnelles le concernant dudit registre. Pour trancher ce litige, la Cour de cassation italienne a demandé à la Cour de justice d'examiner la question de savoir si le principe de conservation des données prévu à l'art. 6, par. 1, let. e, de la directive 95/46/CE, selon lequel les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes pour une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées, doit prévaloir sur le système de publicité des registres de sociétés tel qu'il est prévu par la première directive 68/151/CEE[102].

Selon la Cour de justice, la publicité du registre des sociétés vise à garantir la sécurité juridique entre les sociétés et les tiers et permettre à ces derniers de prendre connaissance des actes essentiels de la société concernée et de certaines données concernant les personnes qui ont le pouvoir de la représenter. La publicité de telles informations est également justifiée après la dissolution d'une société. En effet, il peut s'avérer nécessaire de vérifier par exemple la légalité d'un acte effectué par une société durant son activité, en vue d'une éventuelle action en justice. Or, selon la Cour de justice, les différents régimes de prescription applicables dans les Etats membres rendent impossible la fixation d'un délai unique, à compter de la dissolution de la société, à l'expiration duquel les données enregistrées dans le registre des sociétés ne seraient plus nécessaires. Au vu de ces conditions, la Cour de justice estime que les Etats membres ne sauraient garantir aux personnes concernées, en vertu de l'art. 6, par. 1, let. e, de la directive 95/46/CE, le droit d'obtenir par exemple l'effacement des données les concernant après un certain délai à compter de la dissolution de la société. Néanmoins, si la sécurité juridique et la protection des intérêts des tiers prévalent, il ne saurait être exclu que dans certaines situations particulières et exceptionnelles une personne puisse faire valoir des intérêts prépondérants et légitimes à ce que l'accès aux données la concernant soit limité. La Cour de justice arrive par conséquent à la conclusion qu'il appartient aux Etats membres de déterminer si les personnes concernées peuvent demander à l'autorité chargée de la tenue du registre de vérifier, au cas par cas, s'il est exceptionnellement justifié, pour des motifs prépondérants légitimes, de limiter, à l'expiration d'un délai suffisamment long après la dissolution de la société concernée, l'accès aux données les concernant. S'il est vrai que l'arrêt de la Cour de justice se base sur la directive 95/46/CE qui n'est plus applicable à partir de l'entrée en vigueur du règlement (UE) 2016/679, les considérants de ce jugement restent valables sous la nouvelle législation.

101 Arrêt CJUE du 9 mars 2017, aff. C-398/15, ECLI:EU:C:2017:197 (Manni).

102 Première directive 68/151/CEE du Conseil, du 9 mars 1968, tendant à coordonner, pour les rendre équivalents, les garanties qui sont exigées, dans les Etats membres, des sociétés au sens de l'art. 58 deuxième aliéna du traité, pour protéger les intérêts tant des associés que des tiers, JO L 65 du 14.3.1968, p. 8.

Comme il ressort du principe général fixé à l'art. 9 CC, les registres publics font foi des faits qu'ils constatent et dont l'inexactitude n'est pas prouvée. Vu la finalité de ces registres, le Conseil fédéral considère que des motifs de protection des données ne doivent pas entraver la publicité des registres relatifs aux rapports de droit privé. Il en va de même pour les registres de la propriété intellectuelle: le législateur a procédé lui-même à une pesée des intérêts et garanti la publicité de ces registres. De l'avis du Conseil fédéral, il n'incombe pas au législateur de la protection des données de légiférer sur les droits des personnes concernées dans ces domaines. Il convient par conséquent de prévoir à l'al. 4 une réserve en faveur des dispositions spéciales du droit fédéral. Cette modification ne concerne que les registres publics de droit privé tenus par les autorités fédérales, à savoir le registre informatisé de l'état civil, Zefix, le registre des aéronefs de l'Office fédéral de l'aviation civile et les registres de l'Institut fédéral de la propriété intellectuelle (notamment les registres des marques, des brevets et des designs).

Les registres publics de droit privé qui relèvent de la compétence des cantons sont régis par le droit cantonal de protection des données, y compris lorsque ces données sont traitées en exécution du droit fédéral. Le droit cantonal ne doit toutefois pas empêcher l'application uniforme et juste du droit privé fédéral et en particulier le principe de publicité des registres. L'abrogation de l'art. 2, al. 2, let. d, LPD n'a ainsi pas de conséquences pour les registres cantonaux suivants: le registre foncier, le registre des bateaux, les registres cantonaux du commerce, les registres concernant la poursuite pour dettes et faillites et le registre public sur les pactes de réserves de propriété. Enfin, l'al. 4 n'a aucune conséquence sur les registres publics, qui sont régis par des lois spéciales, et subsidiairement par la LPD, (par ex.: le registre des médecins).

Champ d'application territorial

Le P-LPD ne prévoit pas de disposition particulière concernent le champ d'application territorial de la loi, comme le fait le règlement (UE) 2016/679 (art. 3). Le Conseil fédéral estime que le droit actuel permet déjà d'appliquer la LPD largement à des situations présentant des aspects internationaux, y compris en droit public (en vertu de la théorie des effets[103]).

Les difficultés se situent plutôt du côté de la mise en œuvre et de l'exécution des décisions des autorités, en particulier dans le domaine de l'Internet. Le Conseil fédéral a examiné l'opportunité d'introduire dans la loi l'obligation pour les responsables du traitement et les sous-traitants d'indiquer un domicile de notification en Suisse afin de faciliter l'exécution des décisions les concernant. Il y a renoncé, pour les même raisons que celles évoquées dans son rapport du 11 décembre 2015 sur la responsabilité des fournisseurs de services Internet[104]. Il convient plutôt de favoriser la conclusion de traités bilatéraux ou multilatéraux d'entraide judiciaire prévoyant la

103 S'agissant spécialement de la protection des données, le Tribunal fédéral a retenu, en application de ce principe, que les images prises en Suisse et publiées d'une façon qui permet d'y accéder en Suisse également ont un lien prépondérant avec la Suisse, même si les images sont traitées à l'étranger et ne sont pas mises en ligne directement depuis la Suisse (ATF **138** II 346, consid. 3.3 [«*Google Street View*»]).

104 www.ejpd.admin.ch/dam/data/bj/aktuell/news/2015/2015-12-110/ber-br-f.pdf

transmission directe par voie postale des actes devant être notifiés à l'étranger. Des traités de ce type ont déjà été conclus en matière civile avec quelques Etats qui accueillent le siège social d'exploitants de plateformes bien connus, tels que les Etats-Unis ou l'Irlande. Cette perspective a été confirmée par le Conseil fédéral, dans le domaine pénal, dans sa réponse à la motion Levrat 16.4082 «Faciliter l'accès des autorités de poursuite pénale aux données des réseaux sociaux». Enfin, le Conseil fédéral relève que l'obligation d'élection de domicile est prévue par la PA ainsi que par la LTAF.

Le préposé aurait souhaité que le projet contienne une disposition similaire à l'art. 3 du règlement (UE) 2016/679 et qu'il introduise une obligation, pour le responsable du traitement, d'avoir un représentant en Suisse.

Art. 3 Préposé fédéral à la protection des données et à la transparence

Al. 1 Surveillance par le préposé

L'al. 1 prévoit que le préposé est l'autorité compétente pour surveiller la bonne application des dispositions fédérales de protection des données (cf. art. 39 ss).

Dans le texte allemand, seule la forme masculine de la notion est utilisée lorsque la disposition concerne le préposé en tant qu'institution. C'est le cas le plus fréquent. Dans la première section du chapitre 7 P-LPD (à l'exception de l'art. 42 P-LPD), il est en revanche question du préposé en tant que personne. Pour ces dispositions, le texte allemand utilise alors les formes masculine et féminine du terme.

Al. 2 Dérogations

L'al. 2 exclut plusieurs autorités du champ de surveillance du préposé. Ces dérogations se justifient principalement par le fait que la soumission de ces autorités à cette surveillance serait susceptible de nuire à la séparation des pouvoirs et à l'indépendance de la justice.

Le projet exclut du champ de surveillance du préposé l'Assemblée fédérale (*let. a*) et le Conseil fédéral (*let. b*).

Pour les traitements de données qui tombent dans le champ d'application de la loi, soit les traitements opérés par les services administratifs des tribunaux, il est prévu qu'ils échappent à la surveillance du préposé (*let. c*). Cette exception tient compte du fait que ce dernier pourra à l'avenir rendre des décisions à l'encontre des organes fédéraux. Or, s'agissant des tribunaux fédéraux, cela pourrait mettre en danger leur indépendance, ainsi que le principe de séparation des pouvoirs. Par ailleurs, le Tribunal fédéral et le Tribunal administratif fédéral sont instances de recours contre les décisions du préposé. Ils ne pourraient donc être saisis dans les affaires qui les concernent. Afin de remplir les exigences de la directive (UE) 2016/680 et du P-STE 108, chaque tribunal fédéral va mettre en place une surveillance indépendante, dont la forme et la structure seront analogues à celles du préposé. La mise en place se fera par l'adaptation des ordonnances correspondantes des tribunaux concernés, dès l'entrée en vigueur de la LPD révisée.

Selon la *let. d*, le Ministère public de la Confédération est lui aussi exclu du champ de surveillance du préposé dans la mesure où il traite des données personnelles dans le cadre de procédures pénales[105]. En revanche, les autorités fédérales de police restent soumises à la surveillance du préposé, y compris lorsqu'elles agissent sur ordre du Ministère public de la Confédération. Le préposé applique à cet égard les dispositions en matière de protection des données du droit de procédure applicable (cf. art. 2, al. 3, P-LPD).

Enfin, selon la *let. e*, sont exclues du champ de surveillance du préposé les autorités fédérales dans la mesure où elles traitent des données personnelles dans le cadre de leurs activités juridictionnelles ou dans le cadre de procédures d'entraide judiciaire internationale en matière pénale. Cette exception concerne essentiellement le Ministère public de la Confédération et l'Office fédéral de la justice. Selon la déclaration du Conseil fédéral concernant l'art. 1 de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959[106], l'Office fédéral de la justice doit être considéré comme autorité judiciaire suisse aux fins de la convention. La portée de cette exception est toutefois limitée car le préposé peut vérifier la régularité d'un traitement de données lorsqu'une personne concernée fait valoir les droits qui lui sont consentis par l'art. 11*c* P-EIMP.

9.1.3 Dispositions générales

9.1.3.1 Définitions et principes généraux

Art. 4 Définitions

Let. a Données personnelles

Il convient ici de préciser que le P-LPD utilise en principe la notion de données personnelles. Dans les alinéas, lorsque cela est clair, la notion de données est parfois utilisée comme synonyme.

La définition des données personnelles est modifiée par rapport au droit actuel, dans la mesure où la LPD ne s'applique plus aux personnes morales. Constituent ainsi des données personnelles toutes les informations qui se rapportent à une personne physique identifiée ou identifiable. Est réputée identifiable la personne physique qui peut être identifiée, directement ou indirectement, c'est-à-dire par corrélation d'informations tirées des circonstances ou du contexte (numéro d'identification, données de localisation, éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale). L'identification peut résulter d'un seul élément (numéro de téléphone, d'immeuble, numéro AVS, empreintes digitales) ou du recoupement de plusieurs informations (adresse, date de naissance et état civil). Comme c'est le cas actuellement, une possibilité purement théorique qu'une personne soit identifiée n'est pas suffisante. Ainsi, comme relève le Conseil fédéral dans son message relatif à la LPD de 1988 «si l'identification nécessite des

105 Cf. consid. 80 de la directive (UE) 2016/680 et art. 18 de celle-ci.
106 RS **0.351.1**

moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre (…), on ne peut guère parler de possibilité d'identification»[107]. Il convient de prendre en compte dans chaque cas d'espèce l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne. Le caractère raisonnable des moyens en question doit être évalué au regard de l'ensemble des circonstances, telles que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de leur évolution.

La loi ne s'applique pas aux données qui ont été anonymisées si une ré-identification par un tiers est impossible (les données ont été anonymisées complètement et définitivement) ou ne paraît possible qu'au prix d'efforts tels qu'aucun intéressé ne s'y attèlera. Cette dernière règle vaut aussi pour les données pseudonymisées.

Let. b Personne concernée

La personne concernée est la personne physique dont les données sont traitées. La limitation à la seule personne physique découle de la suppression de la protection des données des personnes morales (cf. commentaire de l'art. 2, al. 1, P-LPD sous ch. 9.1.2).

Let. c Données personnelles sensibles

Le *ch. 1* ne subit pas de modification.

Le *ch. 2* est complété, les données sensibles étant élargies aux données sur l'origine ethnique, comme le prévoient la directive (UE) 2016/680 (art. 10) et le règlement (UE) 2016/679. Le P-LPD conserve la référence à l'origine raciale. Comme c'est le cas pour l'Union européenne, le Conseil fédéral précise que l'utilisation de cette expression n'implique pas qu'il adhère à des théories tendant à établir l'existence de races humaines distinctes. Le projet conserve également la référence aux données relatives à la santé et à la sphère intime. Constituent notamment des données relatives à la sphère intime les données concernant la vie sexuelle et l'orientation sexuelle de la personne concernée (voir aussi la convention STE 108 [art. 6, par. 1] la directive [UE] 2016/680 [art. 10] et le règlement [UE] 2016/679 [art. 9]). L'identité de genre d'une personne est aussi, selon les circonstances, susceptible de tomber dans cette définition (voire dans celle de données relatives à la santé).

La notion de «données sensibles» est par ailleurs élargie aux données génétiques (*ch. 3*) et aux données biométriques identifiant une personne physique de façon unique (*ch. 4*). Cette modification transpose les exigences du P-STE 108 (art. 6, par. 1) ainsi que celles de la directive (UE) 2016/680 (art. 10). Le règlement (UE) 2016/679 prévoit une réglementation identique (art. 9).

Les données génétiques sont les informations relatives au patrimoine génétique d'une personne obtenues par une analyse génétique, y compris le profil d'ADN (art. 3, let. l, de la loi fédérale du 8 octobre 2014 sur l'analyse génétique humaine[LAGH])[108]).

[107] FF **1988** II 452
[108] LAGH; RS **810.12**

Par données biométriques, on entend ici les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment son identification unique. Il s'agit par exemple des empreintes digitales, des images faciales, de l'iris, ou encore de la voix. Ces données doivent impérativement résulter d'un traitement technique spécifique qui permet l'identification ou l'authentification unique d'un individu. Tel ne sera en principe pas le cas, par exemple, de simples photographies.

Let. d Traitement

La définition du «traitement» n'est pas modifiée. La liste a simplement été complétée, par «l'enregistrement» et «l'effacement», dans le but de se rapprocher des textes européens (art. 2, let. b, P-STE 108, art. 4, ch. 2, du règlement (UE) 2016/679 et art. 3, ch. 2, de la directive (UE) 2016/680). La liste des opérations entrant en ligne de compte n'est comme aujourd'hui pas exhaustive, les opérations de traitements pouvant prendre les formes les plus diverses (organisation, structuration, adaptation, extraction de données, etc.). La notion de destruction est plus forte que celle d'effacement et implique que les données soient éliminées irréversiblement. Lorsque les données sont sur papier, ce dernier devra être brûlé ou déchiqueté. Lorsqu'elles sont sur un support informatique, la destruction est plus complexe. Si les données ont été transmises au moyen d'un support tel qu'un CD ou d'une clé USB, il convient de rendre ce dernier inutilisable. Par ailleurs, toutes les copies doivent être traitées de manière à ce que les données ne soient plus lisibles. Si les données personnelles figurent en annexe à un e-mail, les éventuels enregistrements intermédiaires de cet e-mail doivent également être détruits. Les ordres habituels de suppression ou un pur reformatage ne représentent pas une destruction, mais un effacement[109].

L'Union européenne utilise le terme allemand «*verarbeiten*» contrairement au droit suisse qui recourt à la notion de «*bearbeiten*». Pour des raisons pratiques, le projet renonce à modifier la terminologie allemande du droit suisse, ce d'autant plus que ces termes ne présentent aucune différence matérielle.

Let. f Profilage

Le Conseil fédéral propose de supprimer la notion de «profil de la personnalité» telle qu'elle est définie à l'art. 3, let. d, LPD. Ce terme est une spécificité de la législation suisse, qui n'existe pas en droit européen et qui n'est pas connu des législations étrangères. Depuis l'entrée en vigueur de la LPD en 1993, cette notion n'a pas ou peu été appliquée[110] et semble aujourd'hui dépassée par l'évolution technologique. Cette définition est remplacée dans le P-LPD par celle de «profilage», que l'on trouve aussi à l'art. 3, ch. 4, de la directive (UE) 2016/680 et à l'art. 4, ch. 4, du règlement (UE) 2016/679. Les deux notions, bien que présentant de nombreuses similitudes, ne couvrent pas le même état de fait. Le profil de la personnalité est le résultat d'un traitement et traduit ainsi quelque chose de statique. A l'inverse, le pro-

109 Cf. ATAF 2015/13, consid. 3.3.4 et réf.
110 Voir cependant l'arrêt du Tribunal administratif fédéral A-4232/2015 du 18 avril 2017 concernant Moneyhouse AG (ch. 9.1.6).

filage désigne une forme particulière de traitement, et constitue donc un processus dynamique. Ce dernier est par ailleurs toujours orienté vers une finalité particulière.

Compte tenu des avis recueillis lors de la consultation, le terme de profilage est adapté, sur le fond, à la terminologie européenne et ne recouvre plus que le traitement automatisé de données personnelles. Il est défini comme l'évaluation de certaines caractéristiques d'une personne sur la base de données personnelles traitées de manière automatisée, afin notamment d'analyser ou de prédire son rendement au travail, sa situation économique, sa localisation, sa santé, son comportement, ses préférences ou ses déplacements. L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité. Autrement dit, le profilage se caractérise par le fait qu'on procède à une évaluation automatisée de données personnelles afin de pouvoir évaluer, d'une manière également automatisée, les caractéristiques de la personne. On est ainsi en présence d'un profilage uniquement lorsque le processus d'évaluation est entièrement automatisé. On entend par évaluation automatisée toute évaluation fondée sur des techniques d'analyse informatisées. Le recours à des algorithmes est possible mais non constitutif du profilage. En revanche, l'évaluation automatisée des données est indispensable. La simple accumulation de données n'est pas assimilée au profilage. L'évaluation automatisée vise en particulier à analyser ou à prédire certains comportements de la personne. La loi cite quelques exemples de caractéristiques personnelles, telles que le rendement au travail, la situation économique ou la santé. On peut en imaginer d'autres, comme la fiabilité ou le lieu de résidence. Il est sans importance que celui qui procède au profilage le fasse pour lui ou pour le compte d'un tiers.

L'abandon du terme «profil de la personnalité» nécessite l'adaptation des bases légales qui autorisent les organes fédéraux à traiter de tels profils (cf. ch. 9.2.2).

Les données issues d'un profilage sont en principe des données personnelles au sens de l'art. 4, let. a, P-LPD, qui, selon les circonstances, peuvent aussi constituer des données sensibles.

Let. g Violation de la sécurité des données

Contrairement à l'avant-projet, le P-LPD définit la violation de la sécurité des données, la consultation ayant révélé que ce terme manquait de clarté. Est donc considérée comme telle toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non licite ou illicite. Le terme est lié à l'art. 7 P-LPD, selon lequel les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données. La notion correspond à celle des art. 7 P-STE 108, art. 3, ch. 11, de la directive (UE) 2016/680 et art. 4, ch. 12, du règlement (UE) 2016/679.

Ce qui compte, c'est que l'événement en question ait eu lieu. Peu importe que la divulgation ou un accès non autorisés se soient effectivement produits ou aient simplement été rendus possibles. En effet, lorsqu'un support de données a été perdu, il est souvent difficile de prouver que les données qu'il contenait ont été vues ou utilisées par des personnes non autorisées. C'est pourquoi la perte de cet objet cons-

titue en elle-même une violation de la sécurité des données. Ce sont plutôt l'ampleur et la signification d'une telle violation qui sont déterminantes pour les mesures à prendre, en particulier pour l'estimation du risque conformément à l'art. 22, al. 1.

Let. i Responsable du traitement

Le P-LPD prévoit de remplacer la notion de «maître du fichier» par celle de «responsable du traitement», afin d'user de la même terminologie que celle du P-STE 108 (art. 2, let. d), de la directive (UE) 2016/680 (art. 3, ch. 8) et du règlement (UE) 2016/679 (art. 4, ch. 7). Au-delà du fait que la référence au fichier est supprimée, cette modification n'entraîne pas de modification matérielle. Le responsable du traitement, comme le maître du fichier, est celui qui décide des finalités et des moyens (traitement matériel ou automatisé, logiciels mis en œuvre) du traitement des données[111].

Dans le texte allemand seule la forme masculine est utilisée, car le responsable du traitement n'est pas toujours une personne morale.

Let. j Sous-traitant

Il s'agit de la personne privée ou de l'organe fédéral qui traite des données pour le compte du responsable du traitement. Cette notion reprend celle du P-STE 108 (art. 2, let. f), de la directive (UE) 2016/680 (art. 3, ch. 9) et du règlement (UE) 2016/679 (art. 4, ch. 8).

Le contrat liant le responsable du traitement et le sous-traitant peut être de nature diverse. Il peut s'agir d'un mandat (art. 394 ss CO), d'un contrat d'entreprise (art. 363 ss CO) voire d'un contrat mixte selon les obligations du sous-traitant. Le sous-traitant cesse d'être un tiers à compter du moment où il débute ses activités contractuelles pour le compte du responsable du traitement.

Dans le texte allemand seule la forme masculine est utilisée, car le responsable du traitement n'est pas toujours une personne morale.

Définitions non modifiées

Les définitions suivantes ne subissent aucune modification par rapport au droit en vigueur, si ce n'est des adaptations rédactionnelles: «communication» (*let. e*) et «organe fédéral» (*let. h*).

Définitions abrogées

Outre les définitions de profils de la personnalité et de maître du fichier, le projet abroge les définitions suivantes:

– *Fichier:* le P-LPD prévoit de renoncer à cette définition. Cela correspond à la solution retenue par le P-STE 108, qui recourt en lieu et place à la notion de traitement. En effet, compte tenu des nouvelles technologies, les données peuvent aujourd'hui être exploitées comme un fichier, alors même qu'elles sont disséminées. Un exemple parlant est le profilage, lors duquel on va chercher des données dans différentes sources, non constitutives de fichiers,

111 FF **1988** II 455, 456

afin d'évaluer certaines caractéristiques d'une personne. Selon le droit actuel, ces activités échappent aux dispositions de la loi impliquant la présence d'un fichier, comme le droit d'accès (art. 8 LPD) ou le devoir d'information (art. 14 LPD), alors que ce sont justement les situations de ce type qui nécessitent une plus grande transparence. Le Conseil fédéral relève par ailleurs qu'une partie de la doctrine tend à interpréter très largement la notion de fichier, le critère déterminant étant que l'attribution d'une donnée à une personne ne doit pas entraîner d'efforts disproportionnés[112].

– *Loi au sens formel:* le P-LPD propose de supprimer cette définition car elle est superflue.

Art. 5 Principes

Al. 2 Bonne foi et proportionnalité

La version française de l'al. 2 fait l'objet d'une modification rédactionnelle.

Il découle du principe de proportionnalité que seules les données aptes et nécessaires à atteindre les finalités du traitement peuvent être traitées. Par ailleurs, il doit y avoir un rapport raisonnable entre les finalités et le moyen utilisé, les droits de la personne concernée devant être préservés dans la plus large mesure possible (principe de proportionnalité au sens étroit)[113]. Les principes d'évitement et de minimisation des données en constituent deux expressions[114]. Le premier implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée. Le second veut que seules les données absolument nécessaires au but poursuivi soient traitées. Ces deux principes doivent être respectés dès la conception de nouveaux systèmes, et se mêlent ainsi partiellement aux principes de protection des données dès la conception et de protection des données par défaut (cf. commentaire de l'art. 6 P-LPD).

Al. 3 Finalité et reconnaissabilité

L'al. 3 regroupe les principes de finalité et de reconnaissabilité actuellement contenus aux al. 3 et 4 de la loi. Pour mieux aligner le droit fédéral sur le texte du P-STE 108 (art. 5, par. 4, let. b), le P-LPD prévoit que les données doivent être collectées pour des finalités déterminées et reconnaissables pour la personne concernée. Cette nouvelle formulation n'implique pas de changements matériels par rapport au droit en vigueur: tant la collecte des données que les finalités du traitement doivent être reconnaissables. Tel est en principe le cas lorsqu'on informe la personne concernée, lorsque ces traitements sont prévus par la loi ou lorsqu'ils ressortent clairement des circonstances. Le caractère déterminé des finalités implique que des buts vagues, non définis ou imprécis ne suffisent pas. Cette qualité s'apprécie selon les circons-

112 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, nº 563; Belser Urs, in: Maurer-Lambrou/Vogt (éds.), Basler Kommentar, Datenschutzgesetz, 2e éd., Bâle 2006, art. 3 LPD nº 32; VPB 62.57.

113 FF **1988** 458.

114 Baeriswyl Bruno, Commentaire de l'art. 4, in: Beariswyl/Pärli (éds), Datenschutz – Stämpfli Handkommentar, Berne 2015, nº 23.

tances, l'objectif étant de concilier les intérêts des personnes concernées et ceux du responsable du traitement, respectivement du sous-traitant, et de la société.

L'al. 3 mentionne encore que les données doivent être traitées ultérieurement de manière compatible avec les finalités initiales. Cette nouvelle formulation permet de rapprocher la terminologie de la loi avec celle du P-STE 108 (art. 5, par. 4, let. b). Elle n'implique toutefois pas de changements majeurs: comme aujourd'hui, un traitement ultérieur ne sera pas admissible si la personne concernée peut légitimement le considérer comme inattendu, inapproprié ou contestable (voir aussi le ch. 47 du rapport explicatif relatif au P-STE 108 du CAHDATA[115]). On peut citer les cas suivants:

- l'utilisation à des fins publicitaires d'adresses obtenues dans le cadre de la récolte de signatures pour une initiative populaire;
- la collecte et l'analyse d'habitudes de consommation grâce aux paiements effectués par carte de crédit ou carte clients (dans un but qui n'est pas la détection de fraudes), sans le consentement de la personne concernée;
- la collecte et utilisation d'adresses e-mail transmises dans un but déterminé sur Internet par la personne concernée pour l'envoi ultérieur de spams[116];
- la collecte par une entreprises privée d'adresses IP de titulaires de raccordement offrant au téléchargement des œuvres piratées[117].

En revanche, on peut présumer que si la personne concernée transmet son adresse dans le cadre de l'obtention d'une carte client ou pour une commande (en ligne ou non), l'utilisation ultérieure de cette adresse à des fins commerciales par l'entreprise elle-même peut être considérée comme correspondant à une finalité initialement reconnaissable, et donc compatible avec les finalités initiales[118]. Lorsque la modification du but initial est prévue par la loi, requise par un changement législatif ou légitimée par un autre motif justificatif (par ex. le consentement de la personne concernée), le traitement ultérieur est aussi considéré comme compatible avec le but initial.

Al. 4 Durée de conservation des données personnelles

Selon l'al. 4, les données doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement. Cette exigence correspond à ce que prévoit P-STE 108 (art. 5, par. 4, let. e; également le ch. 51 du projet de rapport explicatif relatif au P-STE 108 du CAHDATA), la directive (UE) 2016/680 (art. 4, par. 1, let. e) et le règlement (UE) 2016/679 (art. 5, par. 1, let. e). Elle découle aujourd'hui implicitement du principe général de proportionnalité énoncé à l'al. 2 du présent article. Le Conseil fédéral estime toutefois important, compte tenu des évolutions technologiques et des capacités presque illimitées de stockage, de la mentionner expressément. Le respect de ce principe implique que le responsable du

115 https://rm.coe.int/16806b6ec3
116 JAAC 69.106, consid. 5.6.
117 ATF **136** II 508, consid. 4.
118 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé. Berne 2011, nº 731.

traitement fixe des délais de conservation. Des dispositions spéciales prévoyant des délais de conservation particuliers sont réservées.

Al. 5 Exactitude

L'al. 5 P-LPD reprend le principe de l'exactitude des données figurant actuellement à l'art. 5 LPD, afin de regrouper les grands principes du traitement de données dans une seule disposition, comme le font les textes européens (art. 5 P-STE 108, 4 de la directive [UE] 2016/680 et 5 du règlement [UE] 2016/679). Le terme de «correctes» est remplacé dans le texte français par celui d'«exactes»; en allemand et en italien la terminologie est déjà celle-ci.

Le texte prévoit que celui qui traite des données personnelles doit s'assurer qu'elles sont exactes. Il prend toute mesure appropriée permettant de rectifier, d'effacer ou de détruire les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées. Les données qui ne peuvent être rectifiées ou complétées doivent être effacées ou détruites. L'étendue du devoir d'exactitude doit être déterminée de cas en cas. Elle dépend notamment de la finalité du traitement ainsi que de son ampleur, et du type de données traitées. Le devoir d'exactitude peut impliquer selon les cas de tenir les données à jour.

Certaines obligations légales peuvent s'opposer à la rectification, à l'effacement, ou à la mise à jour des données[119]. Le principe d'exactitude et les devoirs qui y sont liés doivent par ailleurs être aménagés de manière différenciée pour les archives, les musées, les bibliothèques et les autres institutions patrimoniales publiques. Les tâches de ces institutions consistent notamment à collectionner, à répertorier, à conserver et à rendre accessible des documents – numériques ou non – de toutes sortes (art. 2, al. 1, de la loi fédérale du 19 décembre 1992 sur la Bibliothèque nationale suisse[120]). Ces documents ne doivent en eux-mêmes pas être modifiés, car cela irait à l'encontre du but même de l'archivage. Les archives doivent, grâce à ces documents, permettre d'avoir une photo du passé à un moment donné. Leur exactitude se réfère ainsi uniquement à la question de savoir si les documents en question ont été reproduits fidèlement. En d'autres termes, les archives rendent état d'une situation dans le passé, et cela indépendamment du fait de savoir si cette dernière est exacte selon une perspective actuelle. Il existe un intérêt public prépondérant pour cette activité particulière (sur ces questions cf. art. 28, al. 1, let. b, et 37, al. 5, P-LPD et les commentaires y relatifs sous ch. 9.1.6 et 9.1.7).

Al. 6 Consentement

Lorsque le consentement de la personne concernée est requis, celle-ci ne consent valablement, conformément à l'al. 6, que si elle exprime librement et clairement sa volonté concernant un ou plusieurs traitements déterminés et après avoir été dûment informée. La personne concernée accepte donc qu'un traitement de données entraîne une violation de sa personnalité.

119 Comme le devoir de conserver les données intactes, prévu par exemple à l'art. 7 de la loi fédérale du 10 octobre 1997 sur le blanchiment d'argent; RS **955.0**).

120 RS **432.21**

Cette formulation légèrement remaniée permet de se rapprocher de la terminologie du P-STE 108 (art. 5, par. 2), afin de satisfaire aux exigences de celui-ci. Elle ne modifie pas fondamentalement le droit en vigueur. Pour que le consentement soit valable, il faut toujours que le traitement, en particulier son ampleur et son but, soit suffisamment défini. Le consentement peut porter sur plusieurs traitements identiques ou différents. Il est également possible que le but du traitement nécessite plusieurs traitements. A titre d'exemple, un traitement médical peut nécessiter des échanges entre les spécialistes et les services successifs, de même que le traitement de données à des fins de facturation ou de prise en charge par les assurances. Le consentement doit couvrir le but du traitement auquel il sert de motif justificatif. Si les données sont traitées à d'autres fins que celles qui ont fait l'objet d'un consentement, ce traitement doit être justifié par d'autres motifs. Le consentement doit en outre être clair. Il faut donc que la déclaration de la personne concernée exprime la volonté de celle-ci sans ambiguïté. Tout dépend des circonstances concrètes de chaque cas particulier. Conformément au principe de la proportionnalité, on considère aujourd'hui déjà que plus les données sont sensibles, plus le consentement doit être clair[121]. A l'instar du droit en vigueur, le P-LPD ne prévoit pas de forme particulière pour le consentement. En particulier, il n'est pas lié à une déclaration écrite[122]. La personne concernée peut donner un consentement clair au sens de l'al. 6 par la manifestation tacite de sa volonté (cf. art. 1 CO). Tel est le cas lorsque la manifestation de la volonté ne découle pas de la déclaration elle-même, mais d'un comportement qui, compte tenu des circonstances dans lesquelles il se produit, peut être compris comme l'expression claire de la volonté[123]. Exemple: les actes concluants par lesquels la personne concernée manifeste sa volonté, notamment en accomplissant ses obligations contractuelles. Mais la manifestation de la volonté est nécessaire; le simple silence ou l'inaction ne peuvent constituer un consentement valable à la violation de la personnalité[124]. L'art. 6 CO est réservé lorsque les parties sont convenues d'une acceptation tacite.

Selon la seconde phrase de l'al. 6 P-LPD, le consentement doit être exprès lorsque le traitement concerne des données sensibles ou consiste en un profilage. Le consentement au profilage doit satisfaire à des exigences plus élevées, comme c'est actuellement le cas pour le traitement des profils de la personnalité. «Exprès» va plus loin que le consentement «clair» exigé à la 1re phrase de cette disposition. La portée de cette exigence est déjà controversée par certains dans le droit en vigueur[125]. Le Conseil fédéral ne voit cependant pas de raison de s'écarter de la situation juridique actuelle. Pour plus de clarté, le P-LPD remplace, dans les versions française et italienne du texte, les termes de «explicite» et de «*esplicito*», s'agissant de la qualité du consentement concernant les données sensibles, par ceux de «exprès» et «*espresso*», reprenant ainsi la terminologie de l'art. 1 CO. Le texte allemand reste inchangé.

121 FF **2003** 1940
122 Idem
123 Kren Kostkiewicz Jolanta, art. 1, CO, n. 17, *in*: Kren Kostkiewicz Jolanta *et al.* (éditeurs), OR, Schweizerisches Obligationenrecht, Kommentar, 3e édition, Zurich 2016, et les remarques qui s'y trouvent.
124 Hgtaas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Diss. Lucerne, Zurich 2007, n. 393, avec de nombreuses remarques.
125 Cf. Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, *in*: Jusletter, 16 novembre 2015.

Une déclaration de volonté est «expresse» lorsqu'elle est formulée oralement, par écrit ou par un signe, et qu'elle découle directement des mots employés ou du signe en question[126]. Une déclaration de volonté en tant que telle doit manifester clairement la volonté dans sa forme même[127]. Cela pourrait se faire notamment en cochant une case, en optant activement pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration. La même chose vaudrait pour des moyens d'expression non verbaux qui, dans le contexte concret, sont des signes clairs, ou un geste approprié, ce qui peut être fréquemment le cas lors d'une consultation médicale. On peut par exemple penser à des signes approbateurs de la tête ou à l'ouverture de la bouche pour le prélèvement de muqueuse, après des explications claires. Lorsqu'un consentement exprès est requis, il ne peut pas être tacite.

Art. 6 Protection des données dès la conception et par défaut

L'art. 6 P-LPD instaure l'obligation de protéger les données dès la conception et par défaut. Cette obligation étant étroitement liée aux principes de la protection des données, elle est transférée dans les dispositions générales de la loi. Cette disposition met en œuvre les exigences des art. 8bis, ch. 3, P-STE 108 et 20, par. 1, de la directive (UE) 2016/680. L'art. 25 du règlement (UE) 2016/679 contient une règle similaire.

Al. 1 Protection des données dès la conception

L'al. 1 impose au responsable du traitement de concevoir dès l'origine le traitement de données de telle manière qu'il respecte les prescriptions relatives à la protection des données. La nouvelle obligation repose sur le principe de la technologie au service de la protection des données personnelles (*privacy by design*). Le recours à des solutions techniques pour garantir la protection des données s'appuie sur l'idée que la technologie et le droit se complètent. Ainsi, des solutions techniques qui rendent impossible une violation de la protection des données ou qui en réduisent la probabilité rendent les règles juridiques et les codes de conduite moins nécessaires. Par ailleurs, ces technologies sont indispensables pour mettre en œuvre les réglementations de protection des données. Le traitement de données personnelles est omniprésent à bien des égards et va encore s'amplifier (*ubiquitous computing*). Il en résulte des quantités de données personnelles gigantesques, qu'il faut traiter dans le respect des dispositions légales. Or, cela est impossible sans des solutions techniques adaptées. La protection technique des données personnelles ne s'appuie pas sur une technologie précise; elle passe plutôt par la mise en place de règles techniques et organisationnelles conformes aux principes définis à l'art. 5 P-LPD. En d'autres termes, les exigences légales auxquelles doit satisfaire un traitement conforme à la protection des données sont déjà intégrées dans le système, de manière à rendre impossible une

126 ATF **121** III 31, consid. 2c, p. 34; Kren Kostkiewicz Jolanta *et al.* (éditeurs), OR, Schweizerisches Obligationenrecht, Kommentar, 3e édition, Zurich 2016; Gauch Peter/Schluep Walter/Schmid Jörg/Emmenegger Susan, Schweizerisches Obligationenrecht Allgemeiner Teil, vol. 1, 10e édition, Zurich 2014, n. 188.

127 Vasella David, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, *in*: Jusletter, 16 novembre 2015, n. 26 s.

violation de la protection des données ou d'en réduire la probabilité. Il s'agit par exemple de la fixation d'échéances régulières pour l'effacement ou l'anonymisation systématique des données personnelles. Un principe significatif pour la protection des données au plan technique est celui de la minimisation des données, qui ressort aussi de l'art. 5 P-LPD. Selon ce dernier, il faut fixer avant même le début d'un traitement ses modalités, de manière à ce que le moins de données possible soient traitées, et de façon à ce qu'elles soient conservées le moins longtemps possible.

Les organes fédéraux sont aujourd'hui déjà tenus d'annoncer à leurs conseillers à la protection des données, ou au préposé, tous les projets impliquant un traitement automatisé de données. Les exigences de protection des données sont ainsi déjà prises en compte au niveau de la conception des traitements (art. 20 OLPD).

Al. 2 Caractère approprié des mesures

L'al. 2 précise les exigences auxquelles doivent satisfaire les mesures visées à l'al. 1. Ces mesures doivent être appropriées au regard notamment de l'état de la technique, du type de traitement, de son étendue et du degré de probabilité et de gravité du risque que le traitement des données en question présente pour la personnalité et les droits fondamentaux des personnes concernées. Cette disposition se réfère au traitement de données effectué par des acteurs privés et par des organes fédéraux, d'où l'évocation des risques pesant sur la personnalité et sur les droits fondamentaux.

La norme matérialise l'approche fondée sur les risques. Il faut établir un rapport entre le risque induit par le traitement et les moyens techniques permettant de le réduire. Plus le risque est élevé, plus sa survenue est probable, et plus le traitement de données est important, plus les exigences auxquelles doivent répondre les mesures techniques pour être considérées comme appropriées au sens de cette disposition seront élevées.

Al. 3 Protection des données par défaut

Selon l'al. 3, le responsable du traitement est tenu, par le biais de préréglages appropriés, de garantir que le traitement soit limité au minimum requis par la finalité poursuivie, pour autant que la personne concernée n'en dispose pas autrement (*privacy by default*). Les mesures en question résident dans des réglages prédéfinis (par ex. l'installation d'un logiciel) qui s'appliquent de manière standardisée, lorsque l'utilisateur ne choisit pas une autre voie. Ces paramètres standards peuvent être effectués en usine ou ultérieurement (par ex. définir, pour un ordinateur, une imprimante par défaut). Dans le contexte de la protection des données, cela signifie que le processus de traitement doit être préprogrammé de manière à garantir autant que possible la protection des données, mais qu'on laisse à la personne concernée la possibilité d'en modifier les paramètres. Certains sites Internet autorisent par principe les achats sans qu'il faille créer un profil d'utilisateur. Les clients ne fournissent que des informations minimales, soit leur nom et l'adresse de livraison. Ceux qui souhaitent bénéficier de services supplémentaires, tels que l'accès à leur historique d'achat ou à des offres ou la création d'une liste de shopping, doivent consentir à un traitement plus complet de leurs données. Le lien avec la protection des données dès la conception est étroit. En effet, ces réglages prédéfinis s'inscrivent souvent dans un système entier respectueux de la protection des données. Ce qui est spécifique à la protection

des données par défaut, c'est l'influence éventuelle de la personne concernée. Alors qu'elle ne peut en principe pas modifier le système lui-même, elle a toujours la possibilité, s'agissant des réglages par défaut, de choisir une solution différente (cf. art. 5, al. 6, P-LPD). La protection des données par défaut permet en conséquence à la personne concernée de consentir à un traitement déterminé.

La protection des données par défaut joue un rôle mineur dans le secteur public, car les traitements y reposent moins sur le consentement de la personne concernée que sur des obligations légales.

Le responsable du traitement peut montrer, par une certification ou une analyse d'impact relative à la protection des données notamment, qu'il respecte les obligations définies dans cette disposition.

Art. 7 Sécurité des données personnelles

L'art. 7 P-LPD correspond à l'art. 7 LPD, à quelques modifications près. Le devoir d'assurer la sécurité des données est une exigence du P-STE 108 (art. 7) et de la directive (UE) 2016/680 (art. 29). Le règlement (UE) 2016/679 prévoit une règle comparable (art. 32). Les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru. Cette disposition matérialise l'approche fondée sur les risques. Plus le risque d'une atteinte à la sécurité des données est élevé, plus les exigences auxquelles doivent répondre les mesures à prendre seront élevées.

L'*al. 2* mentionne le but des mesures. Ces dernières doivent permettre d'éviter toute violation de la sécurité des données, soit toute violation de la sécurité entraînant la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisés à ces données, et ce indépendamment de la question de savoir si la violation est intentionnelle ou non, licite ou illicite (art. 4, let. g, P-LPD). Les mesures peuvent viser par exemple à pseudonymiser des données, à assurer la confidentialité et la disponibilité du système ou de ses services, ou encore à élaborer des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures prises.

Il existe une interaction entre la protection des données et leur sécurité, mais ces deux aspects doivent être traités séparément. La protection des données relève de la protection de la personnalité de l'individu. Quant à la sécurité des données, elle vise généralement les données présentes chez un responsable du traitement ou chez un sous-traitant et englobe le cadre organisationnel et technique général du traitement des données. Par conséquent, la protection de l'individu n'est possible que si des mesures techniques générales ont été prises pour la sécurité des données le concernant. D'où la distinction opérée entre l'obligation d'assurer la sécurité des données au sens de l'art. 7 P-LPD et la protection des données dès la conception visée à l'art. 6, al. 1, P-LPD. L'art. 7 oblige tant le responsable du traitement que le sous-traitant à prévoir, pour leurs systèmes, une architecture de sécurité appropriée et à les protéger contre les maliciels ou la perte de données, par exemple. L'art. 6, al. 1, par contre, vise à garantir, par des moyens techniques, le respect de prescriptions de protection de données, par exemple la proportionnalité du traitement des données.

Certaines mesures, comme l'anonymisation des données, peuvent à cet égard se révéler significatives pour les deux obligations.

L'*al. 3* oblige le Conseil fédéral à définir des exigences minimales en matière de sécurité des données personnelles.

Art. 8 Sous-traitance

L'art. 8 reprend en substance l'actuel art. 10*a* LPD (traitement des données par un tiers). Les al. 1, 2, et 4 introduisent des modifications terminologiques, rendues nécessaires par les nouvelles définitions (sous-traitant, responsable du traitement). Comme dans le droit actuel, on retiendra que la sous-traitance des données personnelles qui sont protégées par l'art. 321 CP (par ex. les données tombant sous le secret médical) n'est pas exclue par la règle de l'art. 8, al. 1, let. b, P-LPD lorsque le tiers doit être qualifié d'auxiliaire au sens de l'art. 321, al. 1, CP[128]. Si les autres conditions de la sous-traitance sont réunies, il est admis que la personne concernée n'a pas besoin de donner son consentement complémentaire à ce sujet[129].

L'*al. 1* institue un devoir de diligence à la charge du responsable du traitement, dans le but de sauvegarder les droits des personnes concernées en cas de sous-traitance. Le responsable du traitement doit s'assurer de manière active que le sous-traitant respecte la loi dans la même mesure que lui. Cela concerne principalement le respect des principes généraux de protection des données, les règles relatives à la sécurité – expressément mentionnées à l'*al. 2* – ainsi que les règles sur la communication transfrontière. Le responsable du traitement doit, par analogie avec l'art. 55 CO, mettre tout en œuvre pour éviter d'éventuelles violations de la LPD. Il doit ainsi veiller à choisir soigneusement son mandataire, à lui donner les instructions adéquates et à exercer la surveillance nécessaire[130].

L'*al. 3* est nouveau et prévoit que le sous-traitant ne peut lui-même sous-traiter un traitement qu'avec l'autorisation préalable du responsable du traitement. Dans le secteur privé, l'autorisation n'est soumise à aucune exigence de forme. Il appartient toutefois au sous-traitant de prouver l'existence de cette autorisation, si bien qu'il a tout intérêt à la documenter. Dans le secteur public, l'autorisation doit en revanche être écrite. Il s'agit là d'une exigence de la directive (UE) 2016/680, (art. 22, par. 2). Le Conseil fédéral la précisera par voie d'ordonnance. Tant dans le domaine privé que public, l'autorisation peut être spécifique ou générale. Dans cette seconde hypothèse, le sous-traitant informe le responsable du traitement de tout changement (ajout ou remplacement d'autres sous-traitants) lui permettant ainsi, le cas échéant, d'émettre des objections.

128 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, nº 1227 et les références citées.

129 Quelques auteurs sont d'un autre avis: cf. Wohlers Wolfgang, Outsourcing durch Berufsgeheimnisträger, Patienten- und Mandantengeheimnisse als Schranke bei der Auslagerung von Datenverarbeitungen, digma 2016, pp. 114 ss.

130 FF **1988** 421, 470

Les traitements au sein d'une même personne juridique (succursale, unité administrative, employé) ne constituent en principe pas des cas de sous-traitance[131].

Lorsque des données sont stockées «en nuage», il s'agit en principe de sous-traitance, qui doit satisfaire aux conditions y afférentes. Si des données sont transférées à cet effet à l'étranger, il faut en outre que les conditions prévues aux art. 13 et 14 soient remplies.

Art. 9 Conseiller à la protection des données personnelles

L'art. 9 traite du conseiller interne à la protection des données. Le droit en vigueur emploie le terme de «conseiller» en français et celui de «responsable» («*Datenschutzverantwortliche*», «*responsabile*») en allemand et en italien (art. 11*a*, al. 5, let. e, LPD). Pour éviter toute confusion avec le terme «*Verantwortliche*» au sens de l'art. 4, let. i, P-LPD, respectivement avec le mot «*responsabile*» selon l'art. 4, let. j, P-LPD, le P-LPD adopte en allemand et en italien les notions de «*Datenschutzberater*» respectivement «*consulente per la protezione dei dati*», uniformisant ainsi la terminologie dans les trois langues.

Le conseiller à la protection des données veille au respect des prescriptions de protection des données au sein d'une entreprise et prodigue au responsable du traitement des conseils en matière de protection des données. Le responsable du traitement est cependant le seul responsable du traitement en bonne et due forme des données personnelles.

Cette disposition est ajoutée au projet par suite de la consultation, laquelle a révélé le souhait que le conseiller à la protection des données soit explicitement mentionné dans la loi. Le projet va cependant moins loin que le droit européen, qui prévoit dans certains cas une obligation de nommer un tel conseiller. Le préposé aurait souhaité une telle solution. Selon le P-LPD, les entreprises sont libres de nommer ou non un conseiller à la protection des données, alors que les organes fédéraux y sont en principe obligés.

Al. 1 et 2 Désignation

Les responsables du traitement privés peuvent en principe nommer un conseiller à la protection des données à tout moment, comme le dispose l'al. 1. La loi prévoit cependant, eu égard à l'analyse d'impact du traitement, des allégements pour les responsables qui ont nommé un tel conseiller.

L'al. 2 définit les conditions qui doivent être remplies pour que ces allégements s'appliquent (*let. a*). Le projet reprend largement ici le droit en vigueur (cf. art. 12*a* s. OLPD).

Le responsable du traitement peut nommer conseiller à la protection des données un collaborateur ou un tiers. Selon la let. a, le conseiller doit cependant exercer sa fonction de manière indépendante et sans recevoir d'instructions du responsable du traitement. S'il s'agit d'un collaborateur, la hiérarchie en place dans l'entreprise doit

131 Meier Philippe, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, nº 1201. Voir aussi, sur la question de l'employé, le ch. 23 du projet de rapport explicatif du P-STE 108 du CAHDATA.

garantir l'indépendance du conseiller, qui doit en principe être directement subordonné à la direction du responsable du traitement.

La *let. b* renforce encore l'indépendance du conseiller à la protection des données en interdisant à celui-ci d'exercer des tâches incompatibles avec sa mission, ce qui pourrait être le cas, par exemple, s'il était membre de la direction, s'il exerçait des fonctions dans les domaines de la conduite du personnel ou de la gestion des systèmes informatiques, ou s'il appartenait à un service qui traite des données personnelles sensibles. Rien n'interdit en revanche d'imaginer qu'un conseiller à la protection des données puisse être en même temps délégué à la sécurité de l'information.

Selon la *let. c*, le conseiller à la protection des données doit avoir les connaissances professionnelles nécessaires pour exercer cette tâche, s'agissant notamment de la législation en matière de protection des données et des normes techniques relatives à la sécurité des données.

Le conseiller à la protection des données est un interlocuteur important, aussi bien pour la personne concernée que pour le préposé, en ce qui concerne le traitement de données par l'entreprise en question. C'est pourquoi la *let. d* dispose que le responsable du traitement publie les coordonnées du conseiller à la protection des données et les communique au préposé. Une obligation analogue devra être introduite dans l'ordonnance pour les organes fédéraux.

Al. 3 Conseiller à la protection des données d'organes fédéraux

L'al. 3 oblige le Conseil fédéral à régler la désignation d'un conseiller à la protection des données personnelles par les organes fédéraux. Les règles correspondantes figurent principalement dans l'ordonnance, comme c'est le cas dans le droit en vigueur.

Dans l'espace Schengen, les organes fédéraux sont obligés, conformément à l'art. 32 de la directive (UE) 2016/680, de nommer un conseiller (un *délégué*) à la protection des données.

Art. 10 Codes de conduite

Le Conseil fédéral entend encourager l'élaboration de codes de conduite. Ces derniers répondent à un besoin qui a été identifié par l'AIR (cf. ch. 1.8), compte tenu du caractère général de la législation et de son champ d'application personnel et matériel très large. Ces codes permettront de préciser certaines notions, comme le risque élevé (art. 20 P-LPD), ou les modalités de certains devoirs, tels que le devoir d'information (art. 17 à 19 P-LPD) ou celui d'effectuer une analyse d'impact relative à la protection des données (art. 20 P-LPD). L'idée est également de faire émerger des solutions plus précises s'agissant de certains thèmes spécifiques, qui susci-

tent aujourd'hui de nombreuses questions, comme la vidéosurveillance, le *cloud-computing* ou les réseaux sociaux[132].

En permettant aux milieux concernés d'être eux-mêmes actifs en participant à la régulation d'un secteur, le Conseil fédéral entend favoriser l'émergence de solutions de branches, concertées et largement acceptées. Il propose par ailleurs, afin d'inciter à l'autorégulation, que les responsables du traitement qui se soumettent à des codes de conduite puissent, à certaines conditions, renoncer à effectuer une analyse d'impact relative à la protection des données (art. 20, al. 5, P-LPD).

L'encouragement à l'adoption de codes de bonnes pratiques par les Etats et les autorités de contrôle est aussi prévu par le règlement (UE) 2016/679 (art. 40 et 57, par. 1, let. m).

Dans le secteur privé, les codes de conduite doivent émaner des associations professionnelles et des associations économiques que leurs statuts autorisent à défendre les intérêts économiques de leurs membres[133]. Des responsables du traitement et des sous-traitants isolés ne peuvent soumettre leur code au préposé, car l'idée est d'arriver à une certaine standardisation par domaine d'activité. Dans le secteur public en revanche, chaque organe fédéral pourra soumettre le sien. Cela se justifie notamment par la multitude de bases légales applicables et par la variété des tâches des différents organes.

L'*al. 1* prévoit que les codes de conduite peuvent être soumis au préposé. Il ne s'agit pas d'une obligation. Le préposé doit prendre position (al. 2). Le délai dans lequel le préposé doit prendre position dépendra des circonstances du cas d'espèce. Un délai moyen de deux mois devrait pouvoir être respecté.

La prise de position ne constitue pas une décision. Dès lors, les intéressés ne sauraient déduire de droits d'une prise de position positive ni de l'absence de prise de position. Néanmoins, si le préposé donne un avis favorable, il est à présumer qu'un comportement conforme au code de conduite ne fera pas l'objet de mesures administratives par la suite. Les prises de position, qu'elles soient favorables ou non au code de conduite examinés, sont publiées par le préposé.

Le préposé aurait souhaité que l'on introduise une obligation, pour les associations légitimées, de lui soumettre leurs codes. Le Conseil fédéral y a renoncé, compte tenu des résultats de la consultation externe, mais aussi parce que le préposé aurait dû statuer par voie de décision, ce qui aurait entraîné des coûts supplémentaires.

132 A noter que dans le domaine de l'Internet et des télécommunications, les milieux intéressés ont adopté des textes qui, bien que n'étant pas spécialement orientés sur les aspects de protection des données, protègent dans certains cas aussi les droits des personnes concernées. Il s'agit d'une part de la nouvelle initiative sectorielle de l'Association suisse des télécommunications pour une meilleure protection de la jeunesse dans les nouveaux médias et pour la promotion de la compétence en matière de médias dans la société, qui prévoit certaines obligations pour ses signataires concernant le blocage de certains sites Internet et la prise de mesures pour améliorer la protection de la jeunesse dans les nouveaux médias. D'autre part, il s'agit du Code de conduite Hébergement (CCH) de la *Swiss Internet Industry Association* (Simsa) du 1er février 2013, qui est un code de conduite destiné aux fournisseurs suisses de services d'hébergement.

133 Il s'agit de la même notion qu'à l'art. 10, al. 2, LCD.

Art. 11 Registre des activités de traitement

Le P-LPD prévoit, au lieu du devoir de documentation qui figurait dans l'avant-projet, l'obligation de tenir un registre des activités de traitement. La consultation a en effet révélé que la notion de devoir de documentation était trop floue. En outre, le registre des activités de traitement est désormais classé dans les dispositions générales de protection des données, ce qui montre son lien étroit avec les principes de protection des données. L'obligation de tenir un registre remplace l'obligation de déclarer les fichiers qui figure dans le droit en vigueur. La directive (UE) 2016/680 prévoit un tel registre dans son art. 24; le règlement (UE) 2016/679 contient une prescription semblable à l'art. 30.

La tenue du registre incombe, selon l'*al. 1*, au responsable du traitement et au sous-traitant.

L'*al. 2* précise les indications minimales que doit contenir le registre, à commencer par l'identité (le nom) du responsable du traitement (*let. a*) et la finalité du traitement (*let. b*). Le registre doit aussi donner une description des catégories des personnes concernées et des catégories des données personnelles traitées (*let. c*). Par catégories des personnes concernées on entend des groupes partageant les mêmes caractéristiques («consommateurs», «membres de l'armée» ou «employés», par ex). Les catégories des données personnelles traitées désignent la nature des données (données sensibles, par ex.). Le registre doit également indiquer les catégories des destinataires auxquels les données sont susceptibles d'être communiquées (*let. d*). On entend également par là des groupes partageant les mêmes caractéristiques («autorités de surveillance», par ex.). Selon la *let. e*, le registre doit contenir le délai de conservation des données personnelles. Ce délai étant lié, conformément à l'art. 5, al. 4, aux finalités du traitement, il n'est pas toujours possible de l'établir avec précision, d'où la mention «dans la mesure du possible». S'il n'est pas possible de fournir une indication précise, le registre doit au moins indiquer les critères selon lesquels ce délai sera fixé. Selon la *let. f*, le registre doit contenir, si possible, une description générale des mesures visant à garantir la sécurité des données selon l'art. 7. Le but de cette description est de faire apparaître d'éventuels manquements dans les mesures de sécurité. La mention «dans la mesure du possible» indique que cette obligation ne s'applique que si les mesures peuvent être définies de manière suffisamment concrète. Si les destinataires sont à l'étranger, le registre doit permettre de savoir si les conditions d'une communication à l'étranger sont remplies. La *let. g* impose par conséquent le nom de l'Etat et les garanties prises selon l'art. 13, al. 2.

L'énumération de l'al. 2 montre clairement que le registre est un descriptif général des activités de traitement, qui permet de déduire la nature et l'ampleur de celles-ci. Il n'est pas le journal détaillé des traitements effectués par le responsable ou par le sous-traitant. Il fournit, par écrit, les indications importantes relatives à tous les traitements de données d'un responsable du traitement ou d'un sous-traitant. Il permet donc de savoir de manière assez précise si un traitement de données est, en principe, conforme ou non à la protection des données. De plus, le contenu minimal du registre énuméré à l'al. 2 correspond dans une large mesure aux indications que la personne concernée doit recevoir en vertu du devoir d'information et du droit d'accès.

L'*al. 3* contient une liste abrégée des indications minimales devant figurer sur le registre du sous-traitant, dont les catégories de traitements effectués pour le compte du responsable du traitement. Ce registre contient donc aussi l'identité des responsables du traitement pour lesquels le sous-traitant travaille.

Selon l'*al. 4*, les organes fédéraux déclarent leurs registres d'activités de traitement au préposé, lequel, conformément à l'art. 50, tient un registre des activités de traitement des organes fédéraux. Ce registre est rendu public. Pour les organes fédéraux, il n'en résulte aucun changement par rapport au droit en vigueur, car ils ont déjà l'obligation d'élaborer un règlement de traitement et de déclarer leurs fichiers au préposé.

L'*al. 5* permet au Conseil fédéral de dispenser les entreprises qui ont moins de 50 collaborateurs de tenir un registre, le but étant surtout d'alléger la charge des petites et moyennes entreprises. A cet égard, le Conseil fédéral ne tiendra toutefois pas compte uniquement de la taille de l'entreprise mais aussi des risques liés au traitement de données.

Art. 12 Certification

L'art. 12 P-LPD règle la certification facultative, qui figure actuellement à l'art. 11 LPD. En plus des systèmes (procédures et organisation) et des produits (programmes, logiciels, systèmes), il est maintenant possible de faire certifier des services.

Les responsables du traitement qui font l'objet d'une certification sont déliés de leur devoir de procéder à un analyse d'impact relative à la protection des données personnelles (art. 20, al. 5, P-LPD).

La procédure d'accréditation des organismes de certification indépendants par le Service d'accréditation suisse, à laquelle le préposé est associé, demeure inchangée[134].

Le préposé aurait souhaité un système obligatoire pour les traitements à risque élevé. Le Conseil fédéral y a renoncé, dans la mesure où il ne s'agit pas d'une exigence du droit européen.

9.1.3.2 Communications de données personnelles à l'étranger

Art. 13 Principes

Cette disposition correspond aux exigences de l'art. 12 P-STE 108, qui pose le principe selon lequel des données ne peuvent être transmises à l'étranger que si un niveau approprié de protection des données est garanti (par. 2). L'art. 12, par. 3, P-STE 108 définit les cas dans lesquels cette condition est réalisée. L'art. 13 permet aussi de se rapprocher des exigences du droit de l'Union européenne (art. 45 ss du règlement (UE) 2016/679).

134 Ordonnance du 17 juin 1996 sur l'accréditation et la désignation (RS **946.512**) et art. 2 de l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (RS **253.13**).

Les règles relatives aux communications de données personnelles sont en partie remaniées pour tenir compte des résultats de la consultation externe. Le principe selon lequel aucune donnée personnelle ne peut être transmise à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée est supprimé, au motif qu'il crée une insécurité juridique par rapport à la systématique de la réglementation. La terminologie relative aux communications de données personnelles à l'étranger moyennant des garanties appropriées est alignée sur celle du règlement (UE) 2016/679. Les exceptions relatives à la communication de données personnelles vers un Etat dont la législation n'assure pas un niveau de protection des données adéquat sont en outre légèrement assouplies. Enfin, seules les obligations d'informer le préposé ou d'obtenir son approbation, qui sont exigées par le P-STE 108, sont maintenues.

Al. 1 Constatation de l'adéquation par le Conseil fédéral par voie de décision

En vertu de l'al. 1, des données peuvent être communiquées à l'étranger si le Conseil fédéral a constaté que la législation de l'Etat concerné assure un niveau de protection adéquat ou si un organisme international garantit un niveau de protection adéquat. Cette disposition attribue explicitement la compétence au Conseil fédéral d'examiner l'adéquation de la législation étrangère en matière de protection des données.

La situation actuelle est insatisfaisante car il incombe au maître du ficher qui envisage de communiquer des données de vérifier si la législation de l'Etat concerné assure un niveau de protection adéquat[135]. Il peut se référer, le cas échéant, à la liste établie par le préposé, qui énumère les Etats qui remplissent cette exigence (art. 7 OLPD)[136].

Afin de garantir une application uniforme de l'art. 13, le niveau de protection de la législation d'un Etat étranger est dorénavant examiné par le Conseil fédéral. Dans le cadre de son examen, le Conseil fédéral doit non seulement examiner si l'Etat étranger dispose d'une législation remplissant en substance les standards du P-STE 108, mais aussi comment cette législation est mise en œuvre. L'examen du Conseil fédéral peut également porter sur le niveau de protection adéquat garanti par un organisme international. La notion d'«organisme international» vise toute institution internationale, que ce soit une organisation ou une juridiction.

Le résultat de cet examen est publié sous la forme d'une ordonnance du Conseil fédéral, qui est publiée au Recueil officiel. Il conviendra de préciser dans la future ordonnance que le Conseil fédéral devra régulièrement évaluer la situation et que le préposé publiera également sur son site une liste des Etats ou des organismes internationaux pour lesquels le Conseil fédéral a constaté un niveau de protection des données adéquat.

Cette ordonnance est conçue comme une liste «positive» des Etats ayant adopté une législation assurant un niveau de protection adéquat. Si un Etat étranger ne figure

135 FF **2003** 1940-1941

136 La liste du préposé peut être consultée à l'adresse suivante: www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr.

pas dans une ordonnance du Conseil fédéral, cela peut signifier deux choses: soit celui-ci n'a pas encore évalué la législation de ce pays, soit il est arrivé à la conclusion que la loi nationale ne remplit pas les exigences pour qu'il puisse constater un niveau de protection adéquat. Avec la révision, la constatation du Conseil fédéral devient un critère légal pour les responsables du traitement, alors que selon le droit en vigueur la liste du préposé est conçue uniquement comme un moyen auxiliaire mis à la disposition des maîtres du fichier qui envisagent de communiquer des données à l'étranger. Cette solution favorise la sécurité du droit.

Pour son examen, le Conseil fédéral pourra s'appuyer sur les sources disponibles, soit en particulier les évaluations effectuées dans le cadre de la convention STE 108 ou de l'Union européenne. On pourrait également envisager qu'il collabore avec des autorités étrangères et qu'il soit associé à leurs processus d'évaluation.

Lorsque le Conseil fédéral a constaté que la législation d'un Etat ou qu'un organisme international offre un niveau de protection adéquat, la libre circulation des données personnelles de la Suisse vers cet Etat ou cet organisme est garantie, tant pour le secteur privé que pour le secteur public.

Al. 2 Absence de décision du Conseil fédéral

En l'absence d'une décision du Conseil fédéral au sens de l'al. 1, l'al. 2 prévoit que des données personnelles peuvent être communiquées à l'étranger si un niveau de protection approprié est garanti.

En vertu de la *let. a*, le niveau de protection approprié peut être assuré par un traité international. Par «traité international», on entend non seulement une convention internationale en matière de protection des données à laquelle l'Etat destinataire serait partie, telle que la convention STE 108 et son protocole additionnel dont les exigences ont été transposées par l'Etat partie dans son droit interne, mais aussi tout autre accord international qui prévoit un échange de données entre Etats parties et qui répond en substance aux exigences de la convention STE 108. Il peut également s'agir d'un traité international conclu par le Conseil fédéral en vertu de l'art. 61, let. b, P-LPD.

Les let. b à d correspondent aux exigences de l'art. 12, par. 3, let. b, P-STE 108, qui prévoit qu'un niveau de protection des données approprié peut être assuré par des garanties ad hoc et standardisées agrées, établies par des instruments juridiquement contraignants et opposables, conclus et mis en œuvre par les personnels impliquées dans le transfert et le traitement ultérieur des données. Le règlement (UE) 2016/679, à l'art. 46, prévoit une réglementation analogue. Il en va de même de la directive (UE) 2016/680 (art. 37).

Let. b Clauses de protection des données d'un contrat

En vertu de la let. b, des données peuvent être transférées à l'étranger si le responsable du traitement et le cocontractant ont stipulé des clauses de protection des données dans le cadre de leur contrat. La notion de «clauses de protection des données d'un contrat» correspond à la terminologie de l'art. 46, par. 3, let. a, du règlement (UE) 2016/679. Ces clauses doivent préalablement être communiquées au préposé. Dès que cette obligation a été exécutée, les données personnelles peuvent

être communiquées à l'étranger. Le cas échéant, le préposé peut ouvrir une enquête pour établir si ces clauses sont suffisantes. Comme c'est déjà le cas aujourd'hui, il incombe au responsable du traitement de démontrer qu'il a pris toutes les mesures requises pour s'assurer d'un niveau de protection approprié et que le destinataire respecte les clauses contractuelles de protection des données. Contrairement aux clauses type de protection des données (cf. let. d), les clauses de protection des données d'un contrat ne valent que pour les communications prévues dans ledit contrat.

Let. c Garanties spécifiques

Dans le secteur public, l'organe fédéral peut, lorsqu'il accorde sa coopération à un Etat étranger, lui fixer des garanties spécifiques à respecter en matière de protection des données. Il peut par exemple s'agir d'une convention avec l'Etat étranger en question. L'organe fédéral doit préalablement communiquer les garanties au préposé. Dès que cette obligation a été exécutée, les données personnelles peuvent être communiquées à l'étranger.

Let. d Clauses type de protection des données

En vertu de la let. d, des données peuvent être communiquées à l'étranger moyennant des clauses types de protection des données. Cette disposition reprend la terminologie de l'art. 46, par. 2, let. c et d, du règlement (UE) 2016/679. Ces clauses type peuvent être élaborées par les personnes privées, les milieux intéressés ou par des organes fédéraux, ou être établies ou reconnues par le préposé. Les organes fédéraux peuvent également recourir à ce type de garanties. La notion de «clauses type de protection des données» peut viser par exemple des clauses contractuelles standardisées, insérées dans le contrat conclu entre le responsable et le destinataire. Il peut également s'agir d'un code de conduite élaboré par le secteur privé, auxquelles les personnes privées peuvent se soumettre volontairement.

Dans le premier cas, les clauses type de protection des données doivent préalablement avoir été approuvées par le préposé. Cette condition constitue un renforcement du droit en vigueur, qui prévoit uniquement une obligation d'informer le préposé (art. 6, al. 3, LPD). Elle correspond à l'exigence prévue à l'art. 12bis, par. 2, let. b, P-STE 108. Le responsable du traitement ne peut pas recourir aux clauses type de protection des données pour communiquer des données à l'étranger avant d'avoir obtenu une décision du préposé susceptible de recours (art. 5 PA). Durant cette procédure, il peut par contre se prévaloir de l'art. 13, al. 2, let. b ou c. Le délai dans lequel le préposé doit rendre sa décision est régi par l'ordonnance du 25 mai 2011 sur les délais d'ordre[137]. Selon l'art. 4 de cette ordonnance, le délai d'ordre fixé à l'autorité pour prendre sa décision dépend de la complexité de la demande, le délai maximal étant de trois mois.

Dans le second cas, le responsable du traitement peut également recourir aux clauses type de protection des données établies ou reconnues par le préposé, par exemple des contrats-modèles.

Le responsable du traitement qui décide de communiquer des données à l'étranger moyennant des clauses type de protection des données au sens de l'al. 2, let. d, est

137 RS **172.010.14**

présumé avoir pris toutes les mesures nécessaires pour s'assurer un niveau de protection adéquat. Toutefois, cette présomption ne le libère pas de toute responsabilité pour les préjudices qui pourraient résulter de la violation de ces clauses, notamment par le destinataire des données. Il convient de prévoir dans la future ordonnance une obligation pour le préposé de publier une liste des clauses type de protection de données établies ou reconnues, comme le prévoit du reste le droit en vigueur (art. 6, al. 3, OLPD).

Let. e Règles d'entreprise contraignantes

En vertu de la let. e, des données peuvent être communiquées à l'étranger moyennant des règles d'entreprise contraignantes qui ont été préalablement approuvées par le préposé ou par une autorité étrangère chargée de la protection des données. Cette disposition remplace l'art. 6, al. 2, let. g, LPD. L'al. 2, let. e, se rapproche du droit de l'Union européenne, lequel prévoit à l'art. 47 du règlement (UE) 2016/679 que des données peuvent être communiquées entre les entités d'un groupe d'entreprises moyennant des règles d'entreprise contraignantes préalablement approuvées par l'autorité de contrôle de protection des données. L'approbation des règles d'entreprise est prévue à l'art. 57, par. 1, let. s, du règlement (UE) 2016/679. L'al. 2, let. e, constitue un renforcement du droit en vigueur, dans la mesure où les règles d'entreprise contraignantes doivent être approuvées. Le responsable du traitement ne peut pas recourir aux règles d'entreprise contraignantes pour communiquer des données à l'étranger avant d'avoir obtenu une décision du préposé susceptible de recours (art. 5 PA). Durant cette procédure, il peut par contre se prévaloir de l'art. 13, al. 2, let. b ou c.

Pour tenir compte des besoins des groupes d'entreprises situées dans différents pays, l'al. 2, let. e prévoit qu'une entreprise établie en Suisse et appartenant à ce groupe peut également recourir aux règles d'entreprise contraignantes qui ont été approuvées par une autorité étrangère chargée de la protection des données, relevant d'un Etat qui assure un niveau de protection adéquat.

Les instruments visés à l'al. 2, let. e doivent être «contraignants» en ce sens que toutes les sociétés faisant partie d'un même groupe d'entreprises sont tenues de les respecter et de les appliquer. Ces normes doivent préciser les transferts de données, les catégories de données transférées, la finalité, les catégories de personnes et les pays de destination: elles doivent en outre régler les droits des personnes concernées; ces normes doivent enfin préciser les mécanismes mis en place au sein du groupe d'entreprises pour garantir le contrôle du respect de ces normes. Le cas échéant, le Conseil fédéral définira dans le cadre de l'ordonnance d'exécution les critères que doivent remplir les règles d'entreprise contraignantes.

Al. 3 Délégation législative

Cette disposition habilite le Conseil fédéral à prévoir d'autres garanties appropriées au sens de l'al. 2. En effet, il n'est pas exclu que d'autres mécanismes se développent, tels qu'un régime d'autocertification analogue à celui prévu par le *Swiss-US Privacy Shield* (cf. art. 46, par. 2, let. f, du règlement [UE] 2016/679).

Art. 14 Dérogations

Al. 1

A l'instar du droit en vigueur (art. 6, al. 2, LPD), l'al. 1 règle les cas dans lesquels des données peuvent être communiquées à l'étranger en dépit de l'absence d'un niveau de protection adéquat à l'étranger. Il correspond en substance à l'art. 12, par. 4, P-STE 108 et à l'art. 49 du règlement (UE) 2016/679. La directive (UE) 2016/680, à l'art. 38, prévoit une réglementation analogue.

La *let. a* correspond à l'art. 6, al. 2, let. b, LPD, sous réserve que le consentement de la personne concernée doit être donné expressément et que le terme «en l'espèce» est supprimé. Le consentement exprès est une exigence du P-STE 108 (art. 12, par. 4, let. a). On peut sur ce point renvoyer aux explications relatives à l'art. 5, al. 6, P-LPD. La personne concernée doit en particulier connaître le nom de l'Etat tiers (art. 17, al. 4, P-LPD) et être informée des risques du transfert, notamment par rapport au niveau de protection des données de l'Etat étranger. Quant au terme «en l'espèce», le Conseil fédéral considère qu'il peut être supprimé. Comme il résulte de l'art. 5, al. 6, P-LPD, la personne concernée donne son consentement pour un ou plusieurs traitements déterminés. La précision «en l'espèce» est par conséquent superflue.

La *let. b* correspond à l'art. 6, al. 2, let. c, LPD, sous réserve que des données personnelles peuvent être communiquées à l'étranger si la communication est en relation directe avec la conclusion ou l'exécution d'un contrat, non seulement entre le responsable du traitement et la personne concernée mais aussi entre le responsable du traitement et son cocontractant, dans l'intérêt de la personne concernée. L'art. 49, par. 1, du règlement (UE) 2016/ 679 prévoit une disposition analogue.

La *let. c*, ch. 1 correspond au premier cas de figure évoqué à l'art. 6, al. 2, let. d, LPD. Le terme «indispensable» est remplacé dans la phrase introductive de cette let. c par celui de «nécessaire», pour s'aligner sur les textes européens. En ce qui concerne le *ch. 1*, l'existence d'un intérêt public prépondérant doit être attestée par les circonstances du cas d'espèce. Un intérêt purement hypothétique ne suffit pas. Par «sauvegarde d'intérêt public prépondérant» on entend par exemple la sécurité intérieure de la Suisse ou d'un Etat tiers. En vertu de cette disposition, des données personnelles peuvent également être transmises à l'étranger dans le cadre d'actions humanitaires, par exemple lorsqu'il s'agit pour le responsable du traitement de transmettre des données aux fins de recherche des personnes disparues dans une zone de conflit ou dans une région qui a subi une catastrophe naturelle. La *let. c*, ch. 2 correspond au second cas de figure prévu à l'art. 6, al. 2, let. d, LPD, sous réserve que le terme «en justice» qui est jugé trop étroit, est remplacé par «devant un tribunal ou une autorité étrangère compétente».

La *let. d* précise que la communication peut être nécessaire pour protéger la vie ou l'intégrité corporelle non seulement de la personne concernée, mais aussi d'un tiers, pour autant toutefois qu'il ne soit pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable, soit en raison d'une incapacité physique de sa part, soit parce qu'elle n'est pas joignable par exemple par des moyens usuels de communication.

La *let. e* correspond à l'art. 6, al. 2, let. f, LPD.

La *let. f* est une nouvelle disposition. Elle précise que l'exigence d'un niveau de protection adéquat n'est pas applicable lorsqu'il s'agit de communiquer à l'étranger des données provenant d'un registre public prévu par la loi, si certaines conditions légales sont remplies. L'art. 49, par. 1, let. g, du règlement (UE) 2016/679 va dans le même sens en disposant qu'en l'absence d'un niveau de protection adéquat un transfert de données au départ d'un registre est licite s'il est destiné, conformément au droit de l'Union européenne ou de l'Etat membre, à fournir des informations au public, pour autant que certaines conditions légales soient remplies.

Al. 2

Cette disposition prévoit que le préposé peut demander au responsable du traitement ou au sous-traitant de lui communiquer les transferts de données personnelles effectués en vertu de l'al. 1, let. b, ch. 2, c et d. Cette norme correspond aux exigences de l'art. 12, par. 5, P-108. L'avant-dernière phrase du par. 1 de l'art. 49 du règlement (UE) 2016/679 va plus loin, puisqu'il prévoit une obligation pour les responsables du traitement de communiquer spontanément à l'autorité de contrôle les transferts de données personnelles effectués en vertu de l'art. 47 de ce règlement.

Art. 15 Publication de données personnelles sous forme électronique

Cette disposition reprend le contenu de l'art. 5 OLPD. Elle règle la communication de données personnelles par Internet ou par un autre service d'information ou de communication, aux fins d'information du public. Ainsi, il est possible de consulter sur Internet des informations contenant ou non des données personnelles depuis l'étranger, y compris dans un Etat qui ne garantit pas un niveau de protection adéquat des données. La publication de données personnelles sur Internet dans le but d'informer le public, comme c'est le cas par exemple des médias, n'est donc pas assimilée à une communication de données personnelles à l'étranger.

9.1.3.3 Données de personnes décédées

Art. 16

Cette disposition règle différents aspects de la gestion des données d'une personne décédée, laquelle soulève régulièrement des questions pratiques, à commencer par des questions fondamentales: dans quelle mesure la personnalité d'une personne décédée est-elle protégée, et dans quelle mesure y a-t-il lieu de protéger les intérêts éventuels de survivants? Sur le plan constitutionnel, la protection de la personnalité (art. 10 et 13, al. 1, Cst.) perdure après la mort d'une personne, notamment en ce qui concerne les souhaits du défunt quant à ses obsèques[138]. Par contre, la Suisse ne reconnaît pas de droit de la personnalité *post mortem* en tant que tel, qui protège le

138 ATF **129** I 173, consid. 4, et **127** I 115, consid. 4a; SGK-Schweizer, art. 10 Cst., n. 10; BSK-Tschentscher, art. 10 Cst, n. 47 ss. Il n'est pas certain que cela vaille aussi pour l'autodétermination en matière d'information au sens de l'art. 13, al. 2, Cst.

défunt même s'il n'a pas exprimé de volonté à cet égard de son vivant ou s'il n'a pas de parents susceptibles de le défendre[139]. Selon le code civil, la personnalité finit par la mort (cf. art. 31, al. 1, CC)[140]. Mais le Tribunal fédéral estime que dans certains domaines, les effets du droit de la personnalité et de la protection de celle-ci peuvent se prolonger au-delà de la mort[141]. La protection des données ayant pour but la protection de la personnalité, ce principe doit s'appliquer aux données des personnes décédées. En droit pénal, la personnalité est protégée au-delà de la mort, notamment s'agissant de la protection pénale du secret[142].

La gestion des données de personnes décédées n'est actuellement régie que par une seule disposition d'une ordonnance, l'art. 1, al. 7, OLPD, qui fait de la consultation des données d'une personne décédée une modalité du droit d'accès. Or il s'agit d'un droit que la personne concernée ne peut faire valoir que pour les traitements de données qui la concernent personnellement. La disposition de l'ordonnance étend ce droit d'accès à des tiers pour les données d'un autre tiers, sans base légale. L'inscription dans la loi vise à résoudre ce problème. Au point de vue de la systématique, la norme est intégrée aux dispositions générales de protection des données et ne relève plus du droit d'accès, lequel doit rester réservé à la personne concernée. En fait, le projet reprend le droit en vigueur en y apportant les précisions nécessaires sur la forme et sur le fond, et en supprimant les incertitudes existantes. Il veille aussi à ce que la volonté de la personne décédée soit prise en compte le mieux possible.

En plus de régler le droit d'accès aux données d'une personne décédée, la disposition proposée répond en partie au postulat Schwaab 14.3782 «Des règles pour la ‹mort numérique›», en prévoyant à l'al. 2 le droit, pour les héritiers et l'exécuteur testamentaire, d'effacer ou de détruire les données du défunt, c'est-à-dire de provoquer sa mort numérique, sauf si cela va à l'encontre d'un besoin de protection particulier du défunt ou d'intérêts prépondérants du responsable du traitement ou de tiers, ou si le défunt l'a expressément interdit de son vivant. D'autres questions soulevées par le postulat, celle par exemple de la transmissibilité des données, sont en cours d'examen dans le cadre de la révision du droit successoral[143]. Parallèlement à l'art. 16 P-LPD, la révision du droit des successions prévoit un droit de consultation limité aux personnes pouvant fait valoir une prétention successorale (donc patrimoniale). Ce droit leur permet de faire valoir leurs droits patrimoniaux dans le cadre de la dévolution (art. 601*a* AP-CC).

La disposition a été élaguée et précisée par rapport à la version mise en consultation, sans modification notable du contenu. L'art. 12, al. 3, AP-LPD n'a notamment pas été repris, si bien que les dispositions relatives au secret de fonction ou professionnel restent applicables (voir ci-dessous) afin d'éviter des lacunes de protection relevant du droit pénal.

139 Cf. BSK-Tschentscher, art. 10 Cst., n. 47 ss.
140 Cf. ATF **109** II 353, **127** I 145, **129** I 173 et **129** I 302.
141 ATF **129** I 302, consid. 1.2
142 Cf. ATF **135** III 597, **125** IV 298, **118** IV 319 et **118** IV 153.
143 Cf. www.bj.admin.ch/bj/fr/home/gesellschaft/gesetzgebung/erbrecht.html.

Al. 1 Consultation

L'al. 1 dispose que le responsable du traitement accorde la consultation gratuite des données personnelles d'une personne décédée lorsque les trois conditions énumérées aux let. a à c sont remplies.

Selon la *let. a*, la consultation suppose qu'il existe un intérêt légitime ou que le demandeur a un lien de parenté directe avec le défunt ou qu'il était marié, avait conclu un partenariat enregistré ou menait de fait une vie de couple avec lui au moment du décès, ou encore qu'il est son exécuteur testamentaire. Il existe un intérêt légitime justifiant la consultation quand, par exemple, les données en question jouent ou sont susceptibles de jouer un rôle (à titre de preuve, par ex.) dans une procédure concernant le demandeur, ou en relation avec ses propres droits juridiques, en particulier la protection de sa personnalité. La résolution de conflits personnels ou familiaux ou un projet de recherche scientifique peuvent aussi constituer un intérêt légitime. La simple curiosité en revanche, non. Les proches énumérés à la let. a ne doivent, contrairement à toutes les autres personnes, pas faire état d'un intérêt légitime, car leur lien de parenté ou leur relation étroite avec le défunt constitue en soi un intérêt légitime à la consultation des données de celui-ci[144]. Il en va de même pour l'exécuteur testamentaire, qui peut ainsi assumer pleinement sa mission de défense des intérêts du défunt, d'exécution des volontés de celui-ci et en particulier de gestion de l'héritage. Les personnes concernées doivent simplement prouver qu'elles avaient avec le défunt des liens étroits de ce type.

Selon la *let. b*, la consultation n'est possible que si le défunt ne l'a pas interdite expressément et s'il n'a besoin d'aucune protection particulière. La volonté expresse du défunt est toujours prioritaire, ce qui permet de garantir que chacun décide seul de l'accès à ses données personnelles et des personnes autorisées, y compris après sa mort. Une personne peut aussi interdire toute consultation ou la restreindre à certaines personnes ou à certaines données, mais elle doit le faire expressément, comme pour l'art. 26, al. 2, let. b, P-LPD. On peut renvoyer, à cet égard, au commentaire de cet article. Dans la perspective du décès du déclarant, une telle déclaration doit, afin d'être facilement prouvable, revêtir dans la mesure du possible une forme textuelle, par exemple celle d'une directive anticipée ou d'un message clair (écrit ou électronique) adressés directement au responsable du traitement. On peut aussi imaginer une déclaration sous forme de testament. A défaut d'une déclaration expresse du défunt, la consultation peut aussi se heurter au besoin de protection particulière du défunt. Ce peut être le cas lorsqu'un dossier médical ou la correspondance avec un avocat contiennent, par exemple, des données (médicales) spécifiques qui ne font pas partie des indications courantes parce qu'elles concernent la vie sexuelle, certaines maladies, des faits d'inconduite ou encore des transactions juridiques dont on peut supposer que le défunt ne souhaitait pas les rendre publiques ou les communiquer au demandeur.

144 S'agissant de «mener de fait une vie de couple», nous renvoyons en particulier à la doctrine et à la jurisprudence concernant l'art. 165, al. 1, let. a,CPC ou l'art. 10, al. 1, ch. 2, LP.

Selon la *let. c*, la consultation n'est possible que si aucun intérêt prépondérant du responsable du traitement ou d'un tiers ne s'y oppose. Les intérêts de la proche parenté au sens de l'art. 1, al. 7, OLPD sont compris dans les intérêts des tiers. Cette disposition exige une pesée des intérêts: ceux du demandeur, qui souhaite accéder aux données en question, et ceux du responsable du traitement ou de tiers, qui souhaitent que ces données restent secrètes ou du moins qu'elles ne soient pas communiquées au demandeur. Leur caractère prépondérant est décidé au cas par cas, compte tenu du but de la consultation et de l'importance des données pour les personnes impliquées. Les intérêts prépondérants du responsable du traitement qui s'opposeraient à une consultation peuvent être des intérêts personnels, voire une obligation de garder le secret. En pratique, les cas les plus importants sont probablement ceux dans lesquels la consultation s'oppose à des intérêts de tiers. On peut imaginer, par exemple, que la consultation des données révèle que le défunt avait été marié une première fois ou qu'il avait eu un enfant hors mariage. Il faut tenir compte du fait que les personnes ont le droit ne de pas être informées (cf. art. 6 LAGH).

L'art. 16 P-LPD s'applique aussi lorsque la demande de consultation porte sur des données qui sont protégées par le secret professionnel ou de fonction (art. 320 s. CP) du responsable du traitement ou par la disposition pénale de l'art. 56 P-LPD. Imaginons par exemple un fils qui demande à consulter le dossier médical de son défunt père chez le médecin traitant de celui-ci. Certes, l'obligation prévue par le CP de garder le secret professionnel ou de fonction perdure au-delà du décès du maître du secret[145]. On ne peut donc en principe pas forcer le détenteur d'un secret à le révéler. Mais si les conditions de l'art. 16, al. 1, P-LPD sont remplies, un tel détenteur de secret aura le droit d'accorder la consultation des données d'une personne décédée. La révélation constituera alors un acte licite au sens de l'art. 14 CP, et le détenteur du secret ne pourra pas être puni pour violation du secret professionnel ou de fonction. L'art. 16 P-LPD crée ainsi un nouveau motif justificatif pour le détenteur du secret, alors que jusqu'à présent seul le consentement – ou le consentement tacite – du maître du secret était susceptible d'en constituer un.

L'art. 16 P-LPD exige du détenteur du secret une pesée des intérêts qui, dans la plupart des cas, ne devrait poser aucun problème. Si le détenteur du secret se trompe toutefois sur la portée ou sur la réalisation des conditions de l'art. 16, al. 1, P-LPD, il faut examiner s'il n'y a pas erreur sur les faits au sens de l'art. 13 CP ou erreur sur l'illicéité au sens de l'art. 21 CP. Si le détenteur du secret a des doutes par rapport à sa pesée des intérêts et si les conditions de l'art. 16 ne sont pas remplies, il peut y avoir violation par dol éventuel du devoir de garder le secret.

Si le détenteur du secret professionnel ou de fonction doute de la pondération des intérêts, il a en tout cas la possibilité de se faire formellement délier de l'obligation de garder le secret par une autorité compétente au sens de l'art. 320, ch. 2, ou 321, ch. 2, CP. Dans ce cas, c'est l'autorité qui procède à la pesée des intérêts voulue par l'art. 16, al. 1, P-LPD. Le détenteur du secret professionnel ou de fonction ne risque plus d'être puni.

145 ATF **87** IV 105, 107

Lorsqu'un secret professionnel (art. 321 CP) n'est révélé qu'après la mort du maître du secret, des tiers peuvent porter plainte si une loi le prévoit. Ce droit peut aussi résulter d'une autre loi. Lorsqu'une information concerne plusieurs personnes (indications sur une paternité tenue secrète, par ex.), des tiers ont le droit de porter plainte si l'information fait d'eux les maîtres du secret[146].

Si le détenteur du secret a personnellement intérêt à ce que le secret professionnel ou de fonction soit préservé, cet intérêt peut être pris en compte conformément à l'al. 1, let. c.

Les recours en vue de faire valoir le droit à la consultation prévu à l'art. 16, al. 1, P-LPD peuvent, vis-à-vis de responsables du traitement privés, faire l'objet d'une procédure simplifiée conformément à l'art. 243, al. 2, let. d, P-CPC. Cette procédure est aménagée de manière peu compliquée et accessible aux non-juristes («procès civils à caractère social»)[147]. Le juge établit les faits d'office dans les cas visés à l'art. 243, al. 2, CPC (maxime inquisitoire limitée, art. 247, al. 2, let. b, CPC) et intervient de manière plus active dans la procédure. Cela doit aussi permettre à des particuliers d'accéder à un tribunal sans l'aide d'un avocat. La procédure est sans frais en vertu des art. 113, al. 2, let. g, et 114, let. f, P-CPC.

Al. 2 Requête à l'autorité de surveillance

L'al. 2 s'applique au cas où le responsable du traitement est lié par un secret professionnel ou de fonction et qu'il refuse la consultation pour ce motif. Il prévoit que les personnes légitimées selon l'al. 1, let. a peuvent s'adresser aux autorités compétentes selon les art. 320 et 321 CP pour libérer le responsable du traitement de son obligation de secret.

En principe, seul le détenteur du secret, ici le responsable du traitement, peut demander à l'autorité de surveillance ou à l'autorité supérieure de le délier de son obligation de secret professionnel ou de fonction. En effet, il peut avoir besoin de ce motif justificatif. A défaut, son acte pourrait constituer une infraction[148]. En vertu de l'al. 2, un tiers peut également s'adresser directement à l'autorité compétente et requérir la levée du secret. Cette possibilité se justifie dans le cadre particulier de la consultation des données d'une personne décédée. En effet, dans ce cas, le détenteur du secret ne peut être délié par le maître du secret, décédé, à moins que ce dernier ne l'ait fait de son vivant. Cette solution permet de tenir compte de tous les intérêts en présence. Le responsable du traitement peut renvoyer les personnes requérantes à l'autorité de surveillance notamment lorsqu'il a un doute sur la licéité de l'octroi de la consultation. A l'inverse, la consultation des personnes requérantes ne sera pas empêchée pour le seul motif que le responsable ne veut pas demander la levée du secret.

146 Sur toutes ces questions, cf. ATF **87** IV 105, 110; Oberholzer Niklaus, Commentaire bâlois du Code pénal II, Bâle 2013, art. 321, n 34; Riedo Christof, Der Strafantrag, Bâle 2004, 302 ss.

147 Cf. Mazan Stephan, Vorbemerkungen zu Art. 243-247 ZPO, in: Spühler Karl/Tenchio Luca/Infanger Dominik, Commentaire bâlois du Code de procédure civile, 3e éd, Bâle 2017.

148 ATF **123** IV 75, 77, consid. 2b.

L'autorité de surveillance se prononce uniquement sur la question de la levée du secret professionnel ou de fonction, mais cela n'oblige pas le détenteur du secret d'autoriser la consultation des données. S'il devait la refuser malgré la levée du secret par l'autorité, par exemple parce qu'il considère que la personne requérante n'a pas mené de fait une vie commune avec le défunt, la question devrait être réglée sur le plan civil, s'il s'agit d'un responsable du traitement privé, selon le droit de procédure applicable.

Al. 3 Effacement

L'al. 3 dispose que les héritiers et l'éventuel exécuteur testamentaire peuvent exiger que le responsable du traitement efface ou détruise les données personnelles du défunt. Ce droit leur est acquis indépendamment de toute violation de la personnalité ou de tout traitement illicite des données. Il s'agit d'un cas particulier du droit à l'oubli tel que le prévoit l'art. 28 P-LPD pour les vivants.

Ce droit est volontairement limité aux héritiers et à l'exécuteur testamentaire. Contrairement à ce que prévoyait encore le projet mis en consultation, les héritiers ne peuvent faire valoir ce droit que conjointement. Cette modification vise à éviter entre eux tout conflit concernant l'exercice de ce droit. En cas de désaccord, il n'est pas possible d'envisager l'effacement des données du défunt. Autre changement par rapport au projet mis en consultation: le droit est étendu à l'exécuteur testamentaire éventuel.

Selon la *let. a*, l'effacement ou la destruction doivent être refusés si le défunt les a expressément interdits de son vivant. Le but est de respecter la volonté du défunt, qui a pu, par exemple, laisser des instructions sur le destin de ses archives personnelles après sa mort.

L'effacement ou la destruction doivent également être refusés s'ils vont à l'encontre d'intérêts prépondérants du défunt, du responsable du traitement ou de tiers (*let. b*). A cet égard, nous renvoyons au commentaire de l'al. 1, let. b. Contrairement à ce que craignent plusieurs des intervenants s'étant exprimés lors de la consultation, il ne sera donc pas possible aux héritiers d'obliger un responsable du traitement à effacer des données à charge pour un procès. Les intérêts prépondérants du responsable du traitement englobent aussi ses obligations légales s'opposant à un effacement.

Enfin, l'effacement ou la destruction sont exclus s'ils vont à l'encontre d'intérêts publics prépondérants (*let. c*), que peuvent faire valoir tant des responsables du traitement privés que des organes fédéraux. De tels intérêts publics prépondérants peuvent exister en relation avec des documents officiels pour lesquels il existe un droit d'accès en vertu de la LTrans. Il faut aussi signaler les devoirs de conservation imposés par le droit fédéral ou cantonal.

Les actions en justice pour faire valoir le droit à l'effacement prévu à l'art. 16, al. 3, P-LPD à l'encontre des responsables du traitement privés suivent la procédure simplifiée prévue à l'art. 243, al. 2, let. d, P-CPC.

9.1.4 Obligations du responsable du traitement et du sous-traitant

Le chapitre 3 porte sur les obligations du responsable du traitement et du sous-traitant, qui valent tant pour les personnes privées que pour les organes fédéraux.

Art. 17 Devoir d'informer lors de la collecte de données personnelles

L'art. 17 P-LPD regroupe les art. 14, 18 et 18*a* de l'actuelle LPD. Cela permet d'éviter des doublons et d'harmoniser le traitement des données effectué par les organes fédéraux et par les privés. La nouvelle norme remplit les exigences de l'art. 7bis P-STE 108 et de l'art. 13 de la directive (UE) 2016/680. Les art. 13 s. du règlement (UE) 2016/679 contiennent une réglementation similaire.

Le devoir d'informer renforce la transparence des traitements, ce qui est l'un des principaux buts de la révision. En l'absence d'information, la personne concernée ne se rend en effet souvent pas compte que ses données personnelles sont traitées. Par ailleurs, elle ne peut faire valoir les droits que la loi lui accorde que si elle sait que des données la concernant sont traitées. L'amélioration de la transparence du traitement des données personnelles entraîne donc aussi un renforcement des droits de la personne concernée, autre but important de la révision. Enfin, le devoir d'informer contribue à sensibiliser la population sur la protection des données, qui est aussi un objectif de la révision.

Al. 1 Principe

Selon l'al. 1, le responsable du traitement doit informer la personne concernée de la collecte de données personnelles la concernant, que celle-ci soit effectuée auprès d'elle ou non.

Le P-LPD ne précise pas la forme que doit revêtir l'information. Le responsable du traitement doit veiller à ce que la personne concernée puisse effectivement prendre connaissance de celle-ci par un moyen facilement accessible, mais pas à ce qu'elle s'informe effectivement. La possibilité de prendre connaissance des informations varie largement selon que la collecte d'informations est effectuée auprès de la personne concernée ou non.

Une information générale peut suffire si les données sont collectées auprès de la personne concernée (à propos des conditions générales de vente, cf. art. 18, al. 1). On peut recourir à une déclaration standard s'affichant sur un site Internet, mais aussi à des symboles ou à des pictogrammes, pour autant qu'ils contiennent les éléments nécessaires. Si l'on opte pour une information générale, elle doit être facilement accessible, complète et aisément identifiable. Les informations peuvent aussi être données en plusieurs paliers: une vue d'ensemble, puis des informations plus détaillées. La simple indication d'une personne à contacter ne suffit pas. La personne concernée doit pouvoir obtenir les informations sans avoir à les demander.

Si les données personnelles ne sont pas collectées auprès de la personne concernée, le responsable du traitement doit réfléchir à un moyen qui permette à celle-ci de prendre effectivement connaissance de l'information. La simple mise à disposition des informations peut ne pas suffire. Il faut informer activement la personne concer-

née, que ce soit d'une manière générale ou personnalisée. Par exemple, une personne qui n'achète jamais de livres ne se rendra jamais sur le site d'un libraire en ligne pour lire sa déclaration de protection des données. Cette déclaration ne lui apprendra donc pas que le libraire en ligne traite des données la concernant, parce qu'elle n'imagine même pas que cela puisse être le cas. Le devoir d'information vise donc aussi à éviter que des données concernant une personne soient traitées à l'insu de celle-ci. Les exceptions visées à l'art. 18 sont réservées.

L'information n'est soumise à aucune exigence de forme, mais il faut de manière générale en choisir une qui respecte le principe de la transparence des données. Pour des raisons de preuve, il est en outre recommandé de documenter l'information ou d'y procéder par écrit. Par ailleurs, l'information doit être rédigée de manière suffisamment claire pour atteindre son but, à savoir la transparence du traitement des données.

Al. 2 Informations à fournir

La *phrase introductive* de l'al. 2 pose le principe fondamental sur lequel le responsable du traitement doit se baser s'agissant des informations à fournir: il doit communiquer à la personne concernée toutes les informations nécessaires à la mise en œuvre des droits de celle-ci et garantissant la transparence du traitement. Les let. a à c concrétisent ce principe en mentionnant les informations minimales à donner dans tous les cas. Il s'agit (*let. a*) de l'identité, c'est-à-dire du nom et des coordonnées du responsable du traitement, de même que (*let. b*) de la finalité du traitement et, le cas échéant (*let. c*) des destinataires ou des catégories de destinataires auxquels des données personnelles sont transmises. Le responsable du traitement est libre de décider s'il préfère indiquer les destinataires ou les catégories de destinataires. Comme dans l'Union européenne (cf. art. 4, ch. 9, du règlement [UE] 2016/679), les sous-traitants font partie des destinataires au sens de la disposition. Si le responsable du traitement ne souhaite pas révéler l'identité des destinataires, il peut se contenter d'indiquer leur catégorie. Le préposé aurait souhaité que soit également communiquée la base juridique du traitement.

L'association d'une disposition générale définissant les principes de base s'agissant des informations à communiquer (phrase introductive) et d'exigences minimales (let. a à c) permet de mettre en œuvre le devoir d'informer de manière souple. Le degré de détails de l'information dépendra du type de données personnelles traitées ainsi que de la nature et de l'ampleur du traitement. Il est ainsi par exemple possible que l'on doive informer sur la durée du traitement ou l'anonymisation de données. Cette souplesse est nécessaire si l'on veut tenir compte de tous les types de traitements possibles. Elle garantit par ailleurs que seules les informations nécessaires sont transmises. Enfin, elle permet aux responsables du traitement de concrétiser l'obligation d'informer par des codes de conduite adaptés à leur domaine.

Al. 3 Catégories de données personnelles

L'al. 3 dispose que le responsable du traitement doit uniquement communiquer à la personne concernée les catégories de données traitées si les données ne sont pas collectées auprès de celle-ci. Cette restriction découle de l'hypothèse selon laquelle la personne concernée doit avoir au moins connaissance des catégories de données,

voire des données elles-mêmes, si celles-ci ont été collectées auprès d'elle. Dans le cas contraire, elle n'a aucun moyen de savoir quelles catégories de données seront traitées, et il faut les lui indiquer.

Al. 4 Communication de données à l'étranger

Lorsque des données personnelles sont communiquées à l'étranger, le responsable du traitement doit communiquer à la personne concernée le nom de l'Etat tiers destinataire des données. Si l'Etat tiers n'offre pas de protection appropriée et que le responsable du traitement recourt à des garanties au sens de l'art. 13, al. 2, ces garanties doivent être communiquées à la personne concernée. Il en va de même en cas d'application de l'une des exceptions de l'art. 14.

Al. 5 Moment de la communication des informations

L'al. 2 dispose que si les données sont collectées auprès de la personne concernée, la communication des informations requises doit avoir lieu à ce moment-là.

L'al. 5 arrête le moment où la personne concernée doit être informée lorsque les données personnelles ne sont pas collectées auprès d'elle. La disposition fixe pour cela un délai maximal d'un mois. La *2e phrase* prévoit un délai plus court au cas où le responsable du traitement communiquerait les données personnelles à des destinataires avant l'échéance du délai d'un mois: la personne concernée doit alors être informée au moment de la communication. En résumé, le délai est en principe d'un mois à partir de l'obtention des données par le responsable du traitement, quelle que soit la finalité du traitement. Il ne se raccourcit que si le responsable du traitement communique les données à des destinataires.

Art. 18 Exceptions au devoir d'informer et restrictions

L'art. 18 règle les cas où l'obligation d'informer tombe complètement (al. 1 et 2) et ceux où, bien que subsistant en principe, elle peut être limitée (al. 3). Ces deux types de situation sont bien distincts. La norme reprend en partie les règles existantes (art. 9, 14, al. 4 et 5, et 18*b* LPD), qui sont regroupées ici par souci de clarté.

Al. 1 Exceptions générales au devoir d'informer

L'al. 1 définit plusieurs situations dans lesquelles le responsable du traitement est complètement délié de son devoir d'informer la personne concernée.

Selon la *let. a*, le responsable du traitement est délié de son devoir d'information lorsque la personne concernée dispose déjà des informations au sens de l'art. 17. C'est le cas dans différentes configurations. Tout d'abord, il est possible que la personne concernée ait été informée antérieurement et que les informations qui doivent lui être communiquées n'aient pas changé depuis. Ensuite, on peut imaginer que la personne concernée a déjà reçu les informations en vue de son consentement à un traitement de données. Un consentement n'est en effet valable que si la personne concernée a été informée de manière appropriée. Les informations à fournir impérativement sont définies à l'art. 17 et vont même au-delà. Le consentement est régulièrement donné par l'intermédiaire des conditions générales de vente (CGV). Celles-ci peuvent donc en principe servir à informer la personne concernée, sous réserve

qu'elles contiennent les informations nécessaires. Quand la personne a elle-même rendu accessible les données, sans intervention du responsable du traitement (remise d'un dossier de candidature, par ex.), elle est en principe considérée comme informée de la collecte de données.

Selon la *let. b*, le devoir d'informer tombe lorsque le traitement des données personnelles est prévu par la loi, qu'il soit effectué par des organes fédéraux ou par des acteurs privés. De toute façon, les organes fédéraux ne peuvent traiter des données qu'en présence d'une base légale, laquelle fournit régulièrement les informations nécessaires. Il en va de même pour les acteurs privés que la loi oblige à traiter certaines données, par exemple dans la lutte contre le blanchiment d'argent.

Selon la *let. c*, le responsable privé du traitement est délié du devoir d'informer lorsqu'il est soumis à une obligation légale de garder le secret. Cette disposition prévient un conflit de normes en asseyant la primauté du devoir de confidentialité sur le devoir d'information.

Selon la *let. d*, le devoir d'informer tombe aussi lorsque sont remplies les conditions de l'art. 25, qui règle les restrictions au droit d'accès applicable aux médias à caractère périodique. Un privilège analogue est nécessaire s'agissant du devoir d'information des médias, eu égard à la fonction particulière de ceux-ci[149].

Al. 2 Restrictions spécifiques

L'al. 2 prévoit une restriction spécifique du devoir d'information lorsque les données personnelles ne sont pas collectées auprès de la personne concernée. Dans ce cas, le devoir d'informer cette dernière ne s'applique pas si cela est impossible à respecter (*let. a*) ou nécessite des efforts disproportionnés (*let. b*).

L'information est impossible lorsque la personne concernée n'est pas identifiable, par exemple parce qu'il s'agit de la photo d'un inconnu. Cela dit, il ne suffit pas de supposer que l'identification est impossible. Il faut procéder à un minimum de recherches, dans les limites du raisonnable.

Les efforts déployés pour informer la personne concernée sont disproportionnés dès lors qu'ils paraissent injustifiés par rapport au bénéfice que la personne concernée retirerait de l'information. Il faut notamment tenir compte du nombre de personnes concernées. L'information nécessite par exemple des efforts disproportionnés lorsque des données sont traitées uniquement à des fins d'archivage d'intérêt public. L'information de toutes les personnes concernées supposerait régulièrement des efforts considérables, tout en présentant un intérêt souvent limité en raison de l'ancienneté des données, par exemple.

Cette dernière exception doit être interprétée de manière restrictive: le responsable du traitement ne doit pas se contenter d'une supposition. Il doit déployer tous les efforts qu'on est en droit d'attendre de lui dans le cas d'espèce pour remplir son devoir d'information. Ce n'est que si ses efforts restent vains que l'on considérera que l'information n'est pas possible.

149 Cf. Weber Rolf H., Medien im Spannungsfeld von Informationsauftrag und Datenschutz, Jusletter, 8 mai 2017.

Al. 3 Limitation de l'information

L'al. 3 fixe les conditions auxquelles le responsable du traitement peut renoncer à la communication des informations, la restreindre ou la différer. Contrairement aux al. 1 et 2, il englobe les configurations dans lesquelles il y a pesée des intérêts. Les modalités diffèrent selon que le responsable du traitement est un organe fédéral ou un particulier. En fonction de la pesée des intérêts, le responsable du traitement renonce à la communication des informations, la restreint ou la diffère. La liste des cas de limitation est exhaustive et la disposition doit être interprétée restrictivement. L'information ne doit pas être limitée au-delà de ce qui est absolument nécessaire et son motif doit être mis en relation avec l'intérêt à la transparence du traitement. De manière générale, on choisira la solution la plus favorable à la personne concernée, garantissant la transparence maximale du traitement compte tenu des circonstances.

Let. a

La let. a autorise le responsable du traitement à restreindre ou à différer la communication des informations, ou à y renoncer, si les intérêts prépondérants d'un tiers l'exigent. Cette disposition vise en premier lieu les cas dans lesquels les informations concernant le traitement des données personnelles de la personne concernée contiennent aussi des informations sur des tiers. Dans certains cas, les intérêts de ce tiers peuvent être lésés par l'accomplissement du devoir d'information.

Let. b

Selon la let. b, tout responsable du traitement peut restreindre ou différer la communication des informations, ou y renoncer, si l'information compromet les finalités du traitement. Cette exception est à interpréter de manière restrictive. Le responsable du traitement ne peut l'invoquer que si le fait d'informer la personne concernée empêche totalement le traitement d'atteindre son but. Si un traitement poursuit plusieurs buts, la finalité principale est déterminante. Il faut que ce but soit suffisamment important pour justifier une telle restriction du devoir d'informer. Imaginons le cas du journalisme d'investigation, qui ne tombe pas sous le coup de l'exception prévue à l'art. 18, al. 1, let. d, P-LPD. Le devoir d'informer pourrait empêcher un journaliste travaillant sur la révélation d'un scandale politique pour les besoins d'un documentaire d'enquêter sereinement sur les faits. Une telle activité présente aussi un intérêt public considérable, qui justifie une large limitation du devoir d'informer. On peut aussi imaginer que soient traitées, dans le cadre d'une procédure fortement conflictuelle, des données qui ne seront utilisées que dans le courant du procès. Dans ce cas aussi, la communication précoce des données compromettrait complètement les finalités du traitement de celles-ci. D'autant qu'il s'agit ici d'un traitement à caractère unique, tant pour le responsable du traitement que pour la personne concernée, car on suppose, pour l'un comme pour l'autre, qu'ils ne sont pas impliqués dans des procédures judiciaires de ce genre tous les jours. Dans les deux exemples que nous venons d'exposer, le traitement des données présente un grand intérêt et le risque que le devoir d'informer compromette les finalités du traitement est direct et concret. Et dans les deux cas, la personne concernée aura connaissance du traitement au plus tard lors de la publication des données en question, ou lors de leur utilisation dans le procès.

La systématique (inclusion de cette disposition dans l'al. 3) indique que le devoir d'informer demeure le principe. Le responsable du traitement ne peut restreindre ou différer la communication des informations, ou y renoncer, que si celle-ci compromet directement les finalités du traitement. Il doit prendre les mesures les plus favorables du point de vue de la personne concernée, garantissant la transparence maximale du traitement compte tenu des motifs de limitation de l'information.

Il faut bien distinguer l'exception visée à la let. b de celle visée à la let. c. La let. b nécessite une interprétation restrictive et ne peut s'appliquer que si le fait d'informer la personne concernée empêche totalement le traitement d'atteindre son but. Le responsable du traitement ne peut pas l'invoquer au seul motif que l'absence d'information lui paraît plus agréable ou plus pratique. Il ne peut pas non plus l'invoquer de manière systématique, pour l'ensemble de ses activités de traitement. Par ailleurs, les intérêts purement économiques (utilisation des données à des fins publicitaires, par ex.) ne relèvent pas non plus de la let. b. Ce genre d'intérêts du responsable du traitement, moins importants, peuvent, le cas échéant, entrer dans le champ d'application de la let. c.

Let. c

Selon la let. c, un responsable du traitement privé peut restreindre ou différer des informations ou y renoncer si ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à un tiers. Un tel intérêt prépondérant ne doit pas être admis facilement. Il faut effectuer une pesée entre l'intérêt de la personne concernée à être informée d'un traitement de données personnelles afin de faire valoir ses droits, et l'intérêt éventuel du responsable du traitement. Il faut tenir compte de la nature des données personnelles en cause, de leur mode de traitement, du risque d'atteinte à la personnalité et du but du traitement. Il faut au final déterminer si l'information de la personne concernée n'entre pas en conflit avec le but en question, et dans quelle mesure ce dernier est essentiel à l'activité du responsable du traitement.

Let. d

Selon la let. d, un organe fédéral peut restreindre ou différer la communication des données, ou y renoncer, si un intérêt public prépondérant l'exige, en particulier la sûreté intérieure ou extérieure de la Confédération (*ch. 1*). Par sûreté extérieure, on entend, outre le respect des engagements internationaux de la Suisse, la préservation de bonnes relations avec l'étranger. L'organe fédéral peut aussi restreindre ou différer la communication, ou y renoncer, si celle-ci est susceptible de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire (*ch. 2*). Il s'agit d'éviter que la LPD ne permette de contourner les dispositions des codes de procédures, régissant par exemple le droit d'être entendu.

Art. 19 Devoir d'informer la personne concernée en cas de décision individuelle automatisée

L'art. 19 prévoit l'existence d'un devoir d'informer la personne concernée en cas de décision individuelle automatisée. Cette disposition remplit les exigences de l'art. 8, let. a, P-STE 108 et de l'art. 11 de la directive (UE) 2016/680. L'art. 22 du règle-

ment (UE) 2016/679 contient une disposition similaire. L'introduction de la notion de décision individuelle automatisée est nécessaire car ces décisions sont de plus en plus fréquentes en raison du développement technologique.

Al. 1 Information

Selon l'al. 1, le responsable du traitement doit informer la personne concernée de toute décision qui est prise exclusivement sur la base d'un traitement de données personnelles automatisé, y compris le profilage, et qui a des effets juridiques sur la personne concernée ou qui l'affecte de manière significative.

Le Conseil fédéral précisera si besoin dans l'ordonnance dans quels cas une décision est prise exclusivement sur la base d'un traitement de données personnelles automatisé. Cela implique en tout cas qu'il n'y ait eu aucune décision prise par une personne physique sur la base de sa propre évaluation de la situation. Il y a décision individuelle automatisée lorsqu'une exploitation de données a lieu sans intervention humaine et qu'il en résulte une décision, ou un jugement, à l'égard de la personne concernée. Le fait que la décision soit au final communiquée par une personne physique ne change rien à son caractère automatisé, car cette personne n'a pas d'influence sur le processus de décision. La question déterminante est ainsi celle de savoir dans quelle mesure une personne physique peut faire un examen de la situation et se baser sur ses considérations pour rendre une décision finale. Cette décision doit cependant présenter un certain degré de complexité. Les décisions simples du genre de celles qui sont prises lors d'un retrait au bancomat (délivrance du montant demandé si le solde en compte est suffisant) n'en font pas partie.

Il n'est pas nécessaire que la personne concernée soit informée de chaque décision individuelle automatisée, mais seulement lorsque la décision a pour elle des effets juridiques ou l'affecte de manière significative. Ces effets juridiques sont liés, dans le domaine du droit privé, à la conclusion et à la dénonciation de contrats. Il faut à cet égard adopter un point de vue différencié: par exemple, la conclusion d'un contrat d'assurance a des effets juridiques pour la personne concernée. Mais si cette personne reçoit ensuite à intervalles réguliers des avis de paiement de prime, aucun de ces avis ne constitue une décision individuelle avec effets juridiques, car leur émission découle de la conclusion du contrat. Il n'y a pas non plus d'effets juridiques si aucun contrat n'est signé avec la personne concernée. Dans le domaine du droit public, il y a effets juridiques lorsqu'une décision découle d'une décision individuelle automatisée, par exemple une taxation fiscale automatique.

On peut supposer que la personne concernée est affectée de manière significative lorsqu'elle est durablement entravée sur le plan économique ou personnel. Une simple nuisance ne suffit pas. Tout dépend des circonstances concrètes du cas particulier. Il faut en particulier tenir compte de l'importance du bien en question pour la personne concernée, de la durée des effets de la décision et de l'existence ou non d'une solution de remplacement. Selon les circonstances, la personne peut aussi être affectée de manière significative par la non-conclusion d'un contrat. Elle peut également l'être en cas de prestations médicales attribuées sur la base de décisions automatisées.

Le responsable du traitement doit aussi informer la personne concernée en cas de profilage, si celui-ci entraîne une décision qui aura pour elle des effets juridiques

ou qui l'affectera de manière significative. Par exemple, il est possible que la personne concernée soit empêchée d'obtenir une carte de crédit uniquement à cause d'une évaluation négative de sa solvabilité. Cet exemple illustre bien la problématique des décisions individuelles automatisées, car si une évaluation de solvabilité négative peut très bien refléter la situation financière réelle d'une personne, elle peut aussi reposer sur des données fausses ou périmées, en totale contradiction avec la situation réelle de la personne. La décision automatisée affecte alors celle-ci de manière injustifiée.

Al. 2 Exposition du point de vue

Selon l'al. 2, le responsable du traitement doit donner à la personne concernée, si elle le demande, la possibilité de faire valoir son point de vue sur le résultat de la décision, et même de demander comment la décision a été prise. Le but est entre autres d'éviter que le traitement de données soit effectué sur la base de données incomplètes, dépassées ou non pertinentes. Cette règle est également dans l'intérêt du responsable du traitement, pour lequel une décision individuelle automatisée erronée peut avoir des conséquences négatives. Tel est le cas par exemple lorsqu'il refuse de conclure un contrat avec une personne parce que cette dernière est qualifiée par erreur de non solvable. La liberté contractuelle n'en est en rien affectée.

La loi ne précise pas à quel moment la personne concernée doit être informée ni quand elle a la possibilité d'exposer son point de vue. Cela peut donc se faire avant ou après la décision. Il est ainsi notamment possible de lui notifier une décision individuelle automatisée – qui sera désignée comme telle – et de l'entendre dans le cadre de l'exercice du droit d'être entendu, ou lors d'une procédure de recours. Cela ne doit toutefois pas engendrer de frais supplémentaires trop élevés (par ex. des frais de procédure), qui dissuaderaient la personne concernée d'exercer ses droits.

Al. 3 Exceptions

L'al. 3 dispose que le devoir d'informer et d'entendre la personne concernée ne s'applique pas lorsque la décision est en relation directe avec la conclusion ou l'exécution d'un contrat entre le responsable du traitement et la personne concernée et que la demande de cette dernière est satisfaite (*let. a*). Dans un tel cas, on suppose que l'information n'intéresse plus la personne concernée. La demande de cette dernière est satisfaite lorsque le contrat est conclu exactement aux conditions qui figurent sur le devis, par exemple, ou que la personne concernée avait demandées. C'est le cas lorsqu'un contrat de leasing est conclu au taux d'intérêt proposé dans l'offre. Ce n'est pas le cas en revanche lorsque le contrat de leasing est conclu à un taux moins favorable que celui de l'offre, la solvabilité de la personne concernée ayant été jugée insuffisante. Pour que cette disposition s'applique, il faut que la demande de la personne concernée ait été totalement satisfaite. L'obtention de quelques éléments seulement ne suffit pas.

Le devoir d'informer et d'entendre la personne concernée ne s'applique pas non plus lorsque celle-ci a expressément consenti à ce que la décision soit prise de manière automatisée (*let. b*). Cette exception est logique car il faut que la personne concernée ait été informée avant de donner un consentement juridiquement valable.

Al. 4 Décisions individuelles automatisées émanant d'un organe fédéral

L'al. 4 concerne les décisions individuelles automatisées qui émanent d'un organe fédéral. Il s'agit généralement de décisions. L'al. 4 dispose que l'organe fédéral doit signaler ces décisions de sorte que la personne concernée puisse se rendre compte qu'elles n'ont pas été prises par une personne physique. La personne concernée dispose en principe d'un droit de recours. Elle peut donc faire valoir son point de vue et faire examiner la décision par une personne physique. En d'autres termes, les droits garantis par l'art. 19, al. 2, P-LPD le sont déjà par les voies de droit. C'est pourquoi la *2e phrase* de la disposition précise que l'art. 19, al. 2, ne s'applique pas si la personne concernée dispose d'un moyen de recours.

Art. 20 Analyse d'impact relative à la protection des données personnelles

L'art. 20 P-LPD instaure une obligation de procéder à une analyse d'impact relative à la protection des données personnelles. Cette disposition concrétise les exigences posées à l'art. 8bis, par. 2, P-STE 108 et des art. 27 ss de la directive (UE) 2016/680. Les art. 35 s. du règlement (UE) 2016/679 contiennent des dispositions similaires.

La définition et le rôle de l'analyse d'impact résultent de l'al. 20, al. 3 P-LPD. Il s'agit d'un instrument destiné à identifier et à évaluer les risques que certains traitements de données personnelles pourraient entraîner pour la personne concernée. Le cas échéant, cette analyse doit servir à définir des mesures pour faire face à ces risques. L'avantage pour le responsable du traitement est qu'elle permet d'anticiper d'éventuels problèmes juridiques liés à la protection des données et d'éviter les coûts qui pourraient en résulter.

Les organes fédéraux doivent aujourd'hui déjà annoncer les projets impliquant des traitements automatisés de données aux conseillers à la protection des données ou, à défaut, au préposé (art. 20, al. 2, OLPD). Le processus de la méthode de gestion de projets Hermès devrait largement correspondre aux exigences de l'analyse d'impact.

Al. 1 et 2 Motifs justifiant la réalisation d'une analyse d'impact

L'al. 1 prévoit que le responsable du traitement procède à une analyse d'impact lorsque le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée[150]. La règle vaut pour les responsables privés comme pour les organes fédéraux, raison pour laquelle la disposition mentionne un risque élevé non seulement pour la personnalité de la personne concernée, mais aussi pour ses droits fondamentaux. Le responsable du traitement est donc tenu de faire un pronostic des conséquences que le traitement en question peut avoir pour la personne concernée. Sont déterminants, notamment, la nature et l'ampleur de l'impact du traitement sur la personnalité ou les droits fondamentaux de la personne concernée.

Le droit à l'autodétermination en matière informationnelle et le droit à la sphère privée notamment permettent de cerner le risque en question. Ces droits protègent

150 Voir les Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, Working Paper du 4 avril 2017 du Groupe Article 29, pp. 7 ss en particulier.

l'autodétermination de la personne concernée, de même que sa dignité et son identité[151]. Dans le domaine de la protection de données, l'autonomie se traduit principalement par la possibilité de disposer soi-même de ses données personnelles, sans devoir craindre qu'elles ne se trouvent en quantité indéterminée aux mains d'une multitude de tiers pouvant en faire ce qu'ils veulent. Les données sont étroitement liées à l'identité d'une personne. Quiconque dispose de données sur une personne et les combine peut en faire ressortir des détails intimes, qu'elle n'aurait sans doute accepté de révéler qu'à une personne très proche. Ce problème ne concerne pas seulement la liberté de chacun de disposer de ses données personnelles: les données dont on dispose sur une autre personne peuvent influencer de bien des manières ses relations avec son entourage, le cas échéant sans qu'elle en connaisse la raison (par ex. stigmatisation en cas de maladie, restrictions à la conclusion de contrats basées sur l'évaluation de la solvabilité). Le fait de savoir qu'elle est observée peut même amener la personne à modifier son comportement. Enfin, le détenteur des informations pourrait être tenté de les utiliser à des fins susceptibles de porter gravement atteinte à la dignité de la personne concernée.

Pour évaluer le risque, le responsable du traitement doit faire un lien entre, d'une part, le traitement envisagé et, d'autre part, le droit à l'autodétermination informationnelle de la personne concernée ainsi que son droit à sa sphère privée. Il s'agit donc de prendre en considération le traitement des données au regard de l'autodétermination, de l'identité et de la dignité de la personne concernée. On peut admettre l'existence d'un risque élevé lorsqu'il apparaît que les propriétés du traitement envisagé ont – ou pourraient avoir – pour effet de restreindre dans une large mesure la liberté de la personne de disposer de ses données. Ce risque élevé peut résulter, par exemple, de la nature ou du contenu des données à traiter (par ex. données sensibles), de la nature ou de la finalité du traitement envisagé (par ex. profilage), de la quantité de données à traiter, de leur transmission vers un Etat tiers (par ex. si le droit de l'Etat en question ne garantit pas un niveau de protection adéquat) ou de ce que les données seraient accessibles à un grand nombre, voire à un nombre illimité, de personnes.

L'al. 2 précise que l'existence d'un risque élevé dépend de la nature, de l'étendue, des circonstances et de la finalité du traitement. Plus le traitement est étendu, plus les données sont sensibles et plus la finalité du traitement est vaste, plus il y a lieu de conclure à un risque élevé. L'al. 2 mentionne deux exemples dans lesquels un tel risque existe: selon la *let. a*, c'est le cas lorsque le traitement concerne un grand volume de données sensibles, comme cela peut se produire dans le cadre de projets de recherche médicaux. La *let. b* dispose qu'un risque élevé existe en cas de profilage. Tel peut être également le cas lorsque des décisions sont prises exclusivement sur la base d'un traitement de données personnelles automatisé, y compris en cas de profilage, et que ces décisions ont des effets juridiques sur la personne concernée ou l'affectent de manière notable. Il ne faut pas perdre de vue en effet que ce type de décisions peuvent, selon le cas, avoir des répercussions non négligeables pour la personne concernée. Une analyse d'impact est également nécessaire dans de telles situations. Selon la *let. c*, enfin, il y a un risque élevé lorsqu'il s'agit de la sur-

151 Cf. Diggelmann Oliver, in: Waldmann/Belser/Epiney (édit.), Basler Kommentar, Bundesverfassung, Bâle 2015, ad art. 13 Cst. nº 7.

veillance de grandes parties du domaine public (par ex: la surveillance d'un hall de gare).

La *2e phrase* de l'al. 1 autorise le responsable du traitement à effectuer une analyse d'impact commune s'il envisage d'effectuer plusieurs opérations de traitement semblables. Sont visés en particulier les traitements poursuivant un objectif supérieur commun. En pareil cas, il n'est pas nécessaire d'examiner individuellement chacune des étapes prévues sur une plateforme de traitement. L'analyse d'impact peut porter sur la plateforme dans son ensemble.

Al. 3 Contenu de l'analyse d'impact relative à la protection des données personnelles

Selon l'al. 3, l'analyse d'impact relative à la protection des données doit tout d'abord exposer le traitement envisagé. Il faut ainsi présenter les différents processus (par ex. la technologie employée), la finalité du traitement ou la durée de conservation des données personnelles. Par ailleurs, l'analyse d'impact doit montrer quels risques le traitement implique pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'agit ici d'un approfondissement de l'évaluation des risques qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une analyse d'impact. Il convient ainsi de présenter la nature du risque élevé qu'engendre le traitement envisagé et les moyens de l'évaluer. Enfin, l'analyse d'impact doit expliquer les mesures prévues pour faire face à ce risque. Il s'agira souvent de mettre en œuvre les principes de l'art. 5 P-LPD, ainsi que les principes de protection dès la conception et par défaut (*privacy by design*/*by default*; art. 6 P-LPD). A cette occasion, il est possible de mettre en balance les intérêts de la personne concernée et ceux du responsable du traitement. Cette confrontation des intérêts doit être dûment motivée et intégrée dans l'analyse d'impact.

Al. 4 Exceptions en cas d'exécution d'une obligation légale

L'al. 4 dispense les responsables du traitement privés de l'obligation d'établir une analyse d'impact s'ils effectuent le traitement conformément à une obligation légale, par exemple aux fins de la lutte contre le terrorisme ou le blanchiment d'argent. Si le traitement n'a pas de finalité autre que celle prévue par l'obligation légale, on peut partir du principe que le législateur a évalué les risques éventuels pour la personne concernée au regard du but du traitement et édicté, le cas échéant, des prescriptions pour y faire face.

Cette disposition ne s'applique pas en revanche aux traitements effectués par des personnes privées qui n'ont pas pour seul but l'exécution d'une obligation légale. Dans ce cas, le responsable privé doit impérativement procéder à une analyse d'impact relative à la protection des données personnelles.

Al. 5 Exceptions

Les responsables du traitement privés peuvent renoncer à établir une analyse d'impact s'ils possèdent une certification au sens de l'art. 12. La procédure de certification doit inclure le traitement pour lequel il y aurait lieu de procéder à une analyse d'impact.

L'analyse d'impact n'est pas non plus nécessaire si le responsable du traitement privé se conforme à un code de conduite qui satisfait aux exigences de l'al. 5, let. a à c, c'est-à-dire un code de conduite au sens de l'art. 10: concrètement, ce code de conduite doit se fonder sur une analyse d'impact ayant permis d'évaluer les risques que comporte le traitement envisagé (*let. a*). Le code doit prévoir des mesures pour protéger la personnalité et les droits fondamentaux de la personne concernée (*let. b*). Par ailleurs, le code doit avoir été soumis au préposé (*let. c*). On pourrait par exemple imaginer le cas d'une organisation professionnelle d'avocats qui fait développer une plateforme pour la gestion des données de ses clients. Elle procède à cette fin à une analyse d'impact relative à la protection des données et rédige un code de conduite sur la base des résultats de cette analyse. Si un responsable du traitement privé se conforme à ce code de conduite lorsqu'il utilise la plateforme de l'organisation professionnelle, il est dispensé de l'obligation d'établir une analyse d'impact.

Le préposé aurait souhaité que l'exception soit limitée à la certification.

Art. 21 Consultation préalable

A la différence de ce que prévoyait l'avant-projet mis en consultation, la communication au préposé des résultats d'une analyse d'impact relative à la protection des données est traitée dans une disposition propre dans le projet de loi.

Al. 1 Obligation de consulter le préposé

Aux termes de l'al. 1, le responsable du traitement doit obtenir une prise de position du préposé préalablement au traitement s'il ressort de l'analyse d'impact que le traitement envisagé présenterait un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée si aucune mesure n'était prise. Bien qu'elle ne soit pas prescrite par le P-STE 108, cette consultation préalable correspond à la réglementation européenne (art. 28 de la directive [UE] 2016/680 et art. 36 du règlement [UE] 2016/679)[152]. Elle est reprise dans le P-LPD pour permettre au préposé d'exercer une fonction de conseil et de prévention, sans compter qu'elle offre une plus grande efficacité aux responsables du traitement en ce sens que les difficultés qui pourraient surgir en lien avec le traitement sont déjà éliminées à un stade précoce.

Al. 2 et 3 Objections du préposé

Le préposé a deux mois suivant la réception de la communication pour communiquer au responsable du traitement ses objections concernant le traitement et les mesures envisagés. Dans des cas particulièrement compliqués, ce délai peut être prolongé d'un mois. Si le responsable ne reçoit pas de nouvelles du préposé dans le délai de deux mois, il peut partir du principe que le préposé n'a pas d'objections contre les mesures envisagées.

Lorsqu'il est informé du résultat d'une analyse d'impact, le préposé vérifie si les mesures proposées sont suffisantes pour protéger la personnalité et les droits fondamentaux de la personne concernée. S'il arrive à la conclusion que le traitement con-

152 Cf. consid. 94 du règlement (UE) 2016/679.

treviendrait, dans la forme envisagée, aux dispositions de la protection des données, il propose des mesures appropriées au responsable du traitement.

Le préposé n'en reste pas moins libre d'ouvrir une enquête ultérieurement si les conditions de l'art. 43 P-LPD sont remplies, en particulier s'il apparaît que les risques n'ont pas été correctement évalués dans le cadre de l'analyse d'impact et que, par conséquent, les mesures définies ratent leur cible ou sont insuffisantes.

Al. 4 Consultation du conseiller à la protection des données

Le responsable du traitement privé n'est pas tenu de consulter le préposé s'il a nommé un conseiller à la protection des données au sens de l'art. 9 P-LPD et qu'il l'a consulté au sujet de l'analyse d'impact. Le conseiller à la protection des données doit être effectivement intervenu dans l'analyse d'impact. Sa seule nomination ne suffit pas à dispenser le responsable du traitement de l'obligation de consulter le préposé: le conseiller doit jouer un rôle actif dans la réalisation de l'analyse d'impact. Il doit notamment contrôler l'évaluation des risques et les mesures proposées pour faire face aux risques identifiés. Cette disposition vise à alléger la charge des entreprises tout en les encourageant à nommer un conseiller à la protection des données.

Bien que discutée, l'idée d'introduire une exception de ce type dans le règlement (UE) 2016/679 a finalement été abandonnée. Le Conseil fédéral estime qu'il est utile de prévoir ici une exception supplémentaire afin notamment de réduire le travail administratif. Le préposé aurait souhaité que cette exception ne figure pas dans le projet.

Art. 22 Annonce des violations de la sécurité des données

L'art. 22 P-LPD instaure l'obligation d'annoncer toute violation de la sécurité des données personnelles. Cette disposition concrétise les exigences fixées à l'art. 2, par. 2, P-STE 108 et aux art. 30 s. de la directive (UE) 2016/680. Les art. 33 s. du règlement (UE) 2016/679 contiennent des dispositions similaires.

Al. 1 Notion et fondements

L'al. 1 dispose que le responsable du traitement annonce au préposé dans les meilleurs délais toute violation de la sécurité des données entraînant vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. La règle vaut pour les responsables privés comme pour les organes fédéraux, raison pour laquelle la disposition mentionne un risque non seulement pour la personnalité de la personne concernée, mais aussi pour ses droits fondamentaux.

La notion de «violation de la sécurité des données» est définie à l'art. 4, let. g, P-LPD. On entend par là toute violation de la sécurité, sans égard au fait qu'elle soit intentionnelle ou illicite, qui entraîne la perte de données personnelles, leur modification, leur effacement ou leur destruction, ou encore leur divulgation ou un accès non autorisés. La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences ou qui fait preuve de négligence. La violation de la sécurité des données peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Elle peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divul-

gation d'informations que la personne souhaitait garder secrètes. Pour cette raison, l'art. 26, al. 2, let. a, P-LPD considère toute atteinte à la sécurité des données comme une violation de la personnalité.

La personne concernée ne peut réagir à ces menaces que si elle sait que la sécurité des données a été violée. C'est pourquoi le responsable du traitement doit annoncer tout traitement non autorisé au préposé en premier lieu et, si les conditions de l'al. 4 sont remplies, à la personne concernée également. L'annonce doit avoir lieu dans les meilleurs délais à partir du moment où le traitement non autorisé est connu. Le responsable du traitement doit en principe agir rapidement, mais la disposition lui laisse une certaine marge d'appréciation, qui dépend en pratique de l'ampleur du risque pour la personne concernée. Plus ce risque est élevé et le nombre de personnes concernées important, plus son intervention doit être rapide. L'annonce au préposé n'est toutefois nécessaire que s'il est vraisemblable que la violation de la sécurité des données entraînera un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée. Il s'agit d'éviter l'annonce de violations insignifiantes. Le responsable du traitement doit évaluer dans tous les cas les conséquences possibles de la violation pour la personne concernée.

Al. 2 Contenu de l'annonce

L'al. 2 précise les indications que l'annonce au préposé doit contenir au minimum. Le responsable du traitement doit tout d'abord indiquer la nature de la violation, pour autant que cela lui soit possible. On distingue quatre types de violations: l'effacement ou la destruction de données, leur perte, leur modification ou leur communication à des tiers non autorisés. L'annonce doit aussi expliquer, dans la mesure du possible, les conséquences de la violation de la sécurité des données. Ce sont avant tout les conséquences pour la personne concernée et non les conséquences pour le responsable du traitement qui sont visées ici. Enfin, il y a lieu de préciser également les mesures prises ou envisagées pour remédier à la violation de la sécurité des données ou pour atténuer ses conséquences. L'annonce doit permettre dans tous les cas au préposé d'intervenir le plus rapidement et le plus efficacement possible.

Al. 3 Annonce par le sous-traitant

La violation de la sécurité des données peut aussi se produire chez le sous-traitant, qui veille, le cas échéant, à informer le responsable du traitement dans les meilleurs délais de tout traitement non autorisé. Il revient ensuite au responsable du traitement de procéder à une évaluation des risques et de décider si une notification au préposé et à la personne concernée s'impose.

Al. 4 Information de la personne concernée

Selon l'al. 4, la personne concernée ne doit être informée que si les circonstances le requièrent ou que le préposé le demande. Il existe une marge d'appréciation assez large pour déterminer si la première condition est réalisée. Il faut se demander notamment si l'information peut réduire les risques pour la personnalité ou les droits fondamentaux de la personne concernée, en lui permettant notamment de prendre les

dispositions nécessaires pour se protéger (modification des données d'accès ou du mot de passe, par ex.).

Al. 5 Restrictions du devoir d'informer la personne concernée

L'al. 5 dispose que le responsable du traitement peut restreindre l'information de la personne concernée, la différer ou y renoncer dans les cas visés à l'art. 24, al. 1, let. b, et 2, let. b, P-LPD ou si un devoir de secret l'interdit (*let. a*). La *let. b* admet aussi une restriction de l'information s'il n'est pas possible de respecter le devoir d'informer ou que l'information nécessiterait des efforts disproportionnés. Le devoir d'informer est réputé impossible à respecter lorsque le responsable du traitement n'est pas en mesure d'identifier les personnes concernées par la violation de la sécurité des données, par exemple parce que les fichiers journaux qui permettraient une identification ne sont plus disponibles. On estime de même que l'information nécessite des efforts disproportionnés dès lors qu'il faudrait informer individuellement un grand nombre de personnes concernées et que les coûts qui en résulteraient semblent excessifs au regard du gain qu'en retireraient les personnes concernées. C'est notamment dans ces cas de figure que peut s'appliquer la *let. c*: cette disposition autorise le responsable du traitement à opter pour une communication publique si l'information des personnes concernées est garantie de manière équivalente. On estime que cette condition est remplie quand une annonce individuelle ne permettrait pas d'améliorer sensiblement l'information de la personne concernée.

Al. 6 Consentement de la personne soumise à l'obligation d'annoncer

L'obligation d'annoncer les violations de la sécurité des données personnelles inscrite à l'art. 22 P-LPD peut entrer en conflit avec le droit de ne pas contribuer à sa propre incrimination. L'al. 6 prévoit, pour ce type de cas, qu'une annonce effectuée en application de l'art. 22 ne pourra être utilisée dans une procédure pénale engagée contre la personne soumise à l'obligation d'annoncer qu'avec le consentement de celle-ci. La règle vaut aussi bien pour le responsable du traitement que pour le sous-traitant qui annonce une violation de la sécurité des données personnelles.

9.1.5 Droits de la personne concernée

Le chapitre 4 règle les droits de la personne concernée. Le chapitre 5 fixe des dispositions particulières pour le traitement de données par des personnes privées. Le chapitre 6 régit les données traitées par les organes fédéraux.

Art. 23 Droit d'accès

Le droit d'accès complète l'obligation d'informer du responsable du traitement. Il est la clé qui permet à la personne concernée de faire valoir les droits que lui octroie la loi. Le droit d'accès est un droit subjectif inhérent à la personne, que même une personne qui n'a pas l'exercice des droits civils mais qui est capable de discernement peut faire valoir seule, sans avoir à requérir le consentement de son représentant légal. Le fait que ce droit est inhérent à la personne a pour conséquence que nul ne peut y renoncer par avance (art. 23, al. 5, P-LPD).

Al. 1 Principe

L'al. 1 dispose que toute personne peut gratuitement demander au responsable du traitement si des données la concernant sont traitées. Par rapport au droit en vigueur, cette disposition n'a subi que des modifications rédactionnelles.

Al. 2 Informations à communiquer

L'al. 2 dispose que la personne concernée reçoit, lorsqu'elle en fait la demande, les informations qui doivent lui être communiquées conformément au devoir d'informer (cf. art. 17, al. 2, P-LPD). Il s'agit principalement des informations qui sont nécessaires pour que la personne puisse faire valoir ses droits et pour que le traitement des données soit transparent. Cette disposition met en lumière non seulement le lien étroit qui existe entre le droit d'accès et le devoir d'informer, mais aussi le but fondamental du droit d'accès: comme l'a relevé également le Tribunal fédéral[153], le droit d'accès vise à permettre à la personne concernée de faire valoir ses droits en matière de protection des données. Cette précision fait suite aux avis émis par de nombreux participants à la procédure de consultation externe et par certains auteurs, qui critiquent que ce droit d'accès soit souvent utilisé à des fins totalement étrangères à la protection des données[154]. Sont visés en particulier les cas dans lesquels le droit d'accès est utilisé exclusivement dans le but d'obtenir des preuves dans des procès civils qui n'ont aucun lien avec la protection des données. Cette manière de procéder permet de se procurer, sous une forme que l'actuel droit de la procédure ne prévoit pas, des moyens de preuve qu'il y a lieu de qualifier de données personnelles au sens de la LPD, tandis que la collecte des autres moyens de preuve qui ne sont pas des données personnelles doit suivre les voies ordinaires fixées dans le droit de la procédure. Or ces différences dans la manière d'obtenir des preuves ne sauraient se justifier matériellement.

Les let. a à g donnent une énumération non exhaustive des informations qui doivent être communiquées dans tous les cas à la personne concernée. Comme indiqué ci-dessus, il s'agit pour l'essentiel des informations que le responsable du traitement est tenu de lui fournir. La norme générale dans la phrase introductive permet subsidiairement de demander d'autres informations qui sont nécessaires pour que la personne concernée puisse faire valoir ses droits en vertu de la LPD et pour garantir la transparence du traitement. Lorsqu'elle traite des quantités importantes de données sur la personne concernée, la personne tenue de fournir les renseignements doit pouvoir demander à cette dernière de préciser sur quelles données ou quelles opérations de traitement porte sa requête[155].

La personne concernée doit dans tous les cas recevoir des informations sur l'identité et les coordonnées du responsable du traitement (*let. a*). Selon les cas, il est possible qu'elle dispose déjà d'une telle information (dans le cadre du devoir d'information, par ex.). Elle en recevra donc seulement confirmation. Il est toutefois aussi possible que la personne concernée ne connaisse l'identité du responsable du traitement qu'à

153 ATF **138** III 425, consid. 5.3

154 Voir, parmi de nombreux autres, Rosenthal David, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter, 20 février 2017, nº 54 ss.

155 Voir à ce sujet les explications analogues figurant sous le consid. 63 du règlement (UE) 2016/679.

ce moment-là (par ex. en cas de pluralité de responsables du traitement). Par ailleurs, la personne concernée doit être informée des données personnelles traitées (*let. b*) ainsi que de la finalité du traitement (*let. c*). Elle doit également être informée de la durée de conservation des données ou, si cela n'est pas possible, des critères pour fixer cette dernière (*let. d*). Cette information lui permet notamment de savoir si le responsable du traitement conserve les données conformément aux principes de l'art. 5 P-LPD. Comme la durée de conservation des données n'est pas toujours communiquée dans le cadre du devoir d'informer, la personne concernée doit, dans tous les cas, recevoir cette information lorsqu'elle exerce son droit d'accès. Elle reçoit également les renseignements disponibles sur l'origine des données, dans la mesure bien sûr où elle n'a pas fourni elle-même ces données (*let. e*), et est informée, le cas échéant, de l'existence d'une décision individuelle automatisée, ainsi que de la logique sur laquelle se fonde la décision (*let. f*). Il n'y a pas lieu de révéler à la personne les algorithmes utilisés, qui relèvent souvent du secret d'affaires, mais plutôt les hypothèses de base qui sous-tendent la logique algorithmique sur laquelle repose la décision individuelle automatisée. Cela signifie par exemple que la personne doit être informée de ce qu'en raison du résultat négatif de l'examen de sa solvabilité, les conditions qui lui sont proposées pour la conclusion d'un contrat sont moins favorables qu'initialement annoncé. La quantité et la nature des données utilisées pour cet examen, de même que leur pondération respective, doivent en outre être précisées. Enfin, il y a lieu d'indiquer également à la personne concernée les destinataires ou les catégories de destinataires auxquels les données ont éventuellement été communiquées (*let. g*). Si les destinataires se trouvent à l'étranger, l'information doit spécifier l'Etat concerné et, le cas échéant, les garanties prévues au sens de l'art. 13, al. 2, ou l'application d'une des exceptions de l'art. 14.

Al. 3 et 4

Selon l'al. 3, le responsable du traitement peut communiquer à la personne concernée des données sur sa santé par l'intermédiaire d'un professionnel de la santé qu'elle aura désigné. Celui-ci devra posséder les qualifications requises en l'espèce. Reprise du droit en vigueur, cette disposition a été adaptée à la suite des avis exprimés pendant la consultation. Une des adaptations apportées concerne la nécessité d'obtenir le consentement de la personne concernée pour que les données lui soient communiquées par un tiers. Le terme «professionnel de la santé» élargit le cercle des tiers envisageables, offrant ainsi un plus grand choix à la personne concernée.

La *1re phrase* de l'al. 4 est demeurée inchangée. Le responsable du traitement reste en principe tenu de fournir les renseignements demandés lorsque le traitement est effectué par un sous-traitant. Lorsque la personne concernée adresse une demande d'accès directement au sous-traitant, celui-ci doit lui indiquer le nom du responsable du traitement ou transmettre sa demande à ce dernier. S'il n'est pas tenu, en pareil cas, de renseigner lui-même la personne concernée, le sous-traitant ne doit pas non plus entraver l'exercice du droit d'accès. La 2e phrase de l'alinéa est en revanche supprimée.

Al. 5

Cet alinéa correspond à l'actuel art. 8, al. 6, LPD.

Al. 6

L'al. 6 permet au Conseil fédéral de prévoir, dans l'ordonnance, des exceptions à la gratuité. Cette possibilité, qui existe dans le droit en vigueur (cf. art. 2 OLPD), avait été biffée dans l'avant-projet de loi mis en consultation, ce qui avait soulevé de vives oppositions, au motif notamment que l'exception à la gratuité était un moyen de prévenir les invocations abusives du droit d'accès. Suite à ces critiques, la décision a été prise de maintenir la possibilité de prévoir une exception à la gratuité. De cette manière, le Conseil fédéral pourra aussi tenir compte de ce que certaines demandes d'accès occasionnent un volume de travail considérable au responsable du traitement.

Art. 24 Restrictions au droit d'accès

L'art. 24 règle les restrictions au droit d'accès. Hormis quelques adaptations rédactionnelles, les exceptions ont été reprises telles quelles du droit en vigueur.

Al. 1, let. c

Unique disposition nouvelle, la let. c fait suite aux avis émis durant la consultation: elle permet au responsable du traitement de refuser, de restreindre ou de différer la communication des renseignements lorsque la demande d'accès est manifestement infondée ou procédurière. Cette disposition est inspirée, quant au fond, de l'art. 12, par. 5, du règlement (UE) 2016/679, mais reprend la terminologie utilisée en droit suisse, par exemple à l'art. 108 LTF ou aux art. 132 et 253 CPC. Comme il s'agit d'une restriction grave des droits fondamentaux, elle est inscrite dans la loi et non dans l'ordonnance.

L'exception prévue à la let. c doit être interprétée de manière restrictive et ce, à deux égards: d'un côté, le responsable du traitement ne doit pas conclure à la légère au caractère manifestement infondé, voire procédurier, de la demande; de l'autre, c'est à lui qu'il revient de choisir l'option la plus favorable pour la personne concernée dans le cas où la requête serait manifestement infondée ou procédurière. Dans la mesure du possible, il doit se contenter de restreindre la communication des renseignements, mais peut aussi, au besoin, la différer. Le refus de communiquer les informations devra être réservé aux situations dans lesquelles aucun doute n'est permis quant à la nature de la demande. La personne doit dans tous les cas être informée de ce que la communication est refusée, restreinte ou différée (cf. al. 3).

Il n'est pas nécessaire de justifier d'un intérêt ou d'un motif particulier pour invoquer le droit d'accès, la simple curiosité suffit, comme le met en lumière la mention de la transparence du traitement à l'art. 23, al. 2, P-LPD. Le responsable du traitement n'est donc pas habilité à requérir, de manière générale, une motivation. Le Tribunal fédéral a néanmoins relevé que la personne tenue de fournir les renseignements peut demander une justification lorsqu'elle estime être en présence d'une invocation abusive du droit d'accès[156]. Selon la jurisprudence fédérale, une demande d'accès est potentiellement abusive dès lors qu'elle poursuit un but totalement étranger à la protection des données, par exemple économiser les frais liés à l'obten-

156 ATF **138** III 425, consid. 5.4 s., et **123** II 534, consid. 2e.

tion de preuves ou se procurer des informations sur une éventuelle partie adverse[157]. Si l'auteur de la demande fait alors valoir un motif que l'on peut qualifier d'emblée – c'est-à-dire sans clarifications approfondies et de manière certaine – d'infondé, le responsable du traitement peut restreindre la communication. Ce n'est qu'à ces conditions que l'on peut conclure au caractère manifestement infondé du droit d'accès. En d'autres termes, il doit être manifeste que le droit d'accès a été invoqué dans un but qui ne relève aucunement du champ d'application de la LPD ou qu'il vise une finalité tout autre (par ex. intention frauduleuse). S'il n'existe pas de certitude, mais seulement un doute sur la nature de la demande, on ne saurait parler d'une demande manifestement infondée.

La demande d'accès a un caractère manifestement procédurier lorsque le droit d'accès est invoqué de manière répétée sans motif valable ou que la personne adresse sa demande à un responsable dont elle sait pertinemment qu'il ne traite pas de données la concernant. Dans ce cas non plus, le responsable du traitement ne peut pas conclure à la légère à la nature procédurière de la démarche.

Enfin, le responsable du traitement ne peut pas restreindre la communication au sens de l'al. 1, let. c, aux seules fins de préserver ses propres intérêts. Pour se prévaloir de cette possibilité de restriction du droit d'accès, les conditions de l'art. 24, al. 2, let. a, doivent être remplies. La disposition de l'al. 1, let. c, a quant à elle vocation à permettre au responsable du traitement de gérer les demandes qui sont de toute évidence totalement déconnectées du but visé par le droit d'accès.

Le préposé considère que cette exception n'est pas compatible avec la convention STE 108.

Al. 3

Si le responsable du traitement refuse, restreint ou diffère la communication, il doit dûment le motiver en vertu de l'al. 3. Il ne peut invoquer en principe que les motifs prévus aux al. 1 et 2. Dans ce cas, les organes fédéraux doivent rendre des décisions susceptibles de recours. Les responsables du traitement privés ne sont en revanche pas soumis à des exigences de forme. Pour des raisons de preuve, les motifs devraient toutefois être communiqués par écrit à la personne concernée.

La motivation doit permettre à la personne concernée de vérifier si la restriction de son droit d'accès est justifiée. Le degré de motivation ne doit cependant pas être trop élevé si cela est incompatible avec le motif justifiant le refus.

Art. 25 Restrictions au droit d'accès applicable aux médias

L'art. 25 P-LPD reprend l'actuel art. 10 LPD, consacré aux restrictions du droit d'accès applicable aux médias. Il n'y a pas de changement matériel. Le critère de la publication dans la partie rédactionnelle d'un média demeure. Ce critère implique que seules les données rassemblées dans le but de faire paraître un travail journalistique «dans la partie du média réservée aux contributions rédactionnelles» sont concernées; les données doivent servir exclusivement à ce but et non, par exemple, à

157 ATF **138** III 425, consid. 5.5

la promotion de l'entreprise de média[158]. On considère comme média à caractère périodique les journaux, les revues, les émissions de radio et de télévision, les agences de presse et les services d'information en ligne mis à jour et consultés périodiquement, autrement dit, les services offerts sur Internet, s'ils sont renouvelés à la manière d'un périodique, selon un rythme régulier connu du public[159].

9.1.6 Dispositions particulières pour le traitement de données personnelles par des personnes privées

Le chapitre 5 fixe des normes spécifiques applicables aux personnes privées. Les dispositions particulières pour le traitement de données par des personnes privées concrétisent la protection de la personnalité visée à l'art. 28 CC en matière de protection des données. Elles contribuent ainsi à la réalisation du droit à l'autodétermination en matière informationnelle dans les relations entre privés (cf. art. 35, al. 1 et 3, Cst.). Les trois dispositions de cette section sont à considérer ensemble: l'art. 26 P-LPD concrétise les atteintes à la personnalité lors du traitement des données, l'art. 27 P-LPD définit les motifs justificatifs et l'art. 28 P-LPD règle les droits que les victimes d'un traitement ayant porté atteinte à leur personnalité peuvent faire valoir. Le projet reprend dans une large mesure les dispositions existantes, moyennant quelques adaptations rédactionnelles destinées à les rendre plus claires.

L'évaluation de la LPD a par ailleurs montré que les personnes concernées font rarement valoir leurs droits, en particulier dans le secteur privé. Ce comportement est mis sur le compte des craintes concernant le coût que peut avoir un procès[160], craintes qui ont incité à revoir la répartition des coûts en procédure civile (9.2.15).

Art. 26 Atteintes à la personnalité

L'art. 28 CC ne définit pas la notion d'atteinte à la personnalité. L'art. 26 P-LPD concrétise cette notion par rapport aux atteintes à la personnalité causées par un traitement de données.

Al. 1 Principe

L'al. 1 prescrit qu'un traitement de données ne doit pas porter une atteinte illicite à la personnalité de la personne concernée. Il reprend mot pour mot la norme en vigueur. Le droit de disposer de ses propres données personnelles, protégé par le droit à l'autodétermination en matière informationnelle, peut vite être limité par un traitement de données. Il est donc primordial que les personnes privées, qui effectuent une bonne part des traitements, respectent les principes de protection des données.

158 Barrelet Denis/Werly Stéphane, Droit de la communication, 2e éd., Berne 2011, no 1769.
159 Barrelet Denis/Werly Stéphane, Droit de la communication, 2e éd., Berne 2011, no 1420.
160 Cf. pp. 90 ss et 219 du rapport intitulé «Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011» (disponible uniquement en allemand).

Al. 2 Cas d'atteintes à la personnalité

L'al. 2 se réfère notamment au respect des principes applicables aux traitements des données et prévoit trois cas de figure où il y a atteinte à la personnalité.

La *let. a* dispose qu'il y a atteinte à la personnalité lorsque le responsable du traitement traite des données en violation des principes définis aux art. 5 et 7.

La *let. b* ajoute comme cas de figure le fait de traiter des données personnelles contre la manifestation expresse de la volonté de la personne concernée. Il découle de cette disposition que la personne concernée a le droit d'interdire expressément un certain traitement, sans avoir à remplir d'autres conditions (*opting-out*). Cette possibilité, qui existe déjà dans le droit en vigueur, est aussi prévue à l'art. 8, let. d, P-STE 108. Une manifestation de volonté est expresse lorsqu'elle résulte de mots écrits ou parlés, ou découle d'un signe, et que la volonté exprimée résulte directement de ces mots ou de ce signe. La personne concernée doit exprimer directement par des mots ou des signes qu'elle n'est pas d'accord avec un traitement de données particulier. La manifestation de volonté en tant que telle doit, par la manière dont elle est exprimée, déjà clarifier la volonté. La personne concernée devrait ainsi par exemple résilier un service qui implique un traitement de données ou faire une déclaration écrite ou orale indiquant au responsable du traitement qu'elle ne veut pas que ses données soient traitées. Une manifestation de volonté «tacite» n'est ici pas suffisante (cf. le commentaire de l'art. 5, al. 6, P-LPD au ch. 9.1.3.1). Tel est le cas par exemple lorsque la personne concernée n'utilise simplement plus un service impliquant un traitement de données.

Selon la *let. c*, il y a également atteinte à la personnalité lorsque des données sensibles sont transmises à des tiers.

L'énumération n'est pas exhaustive. En d'autres termes, un autre cas de figure de traitement que ceux mentionnés ci-dessus peut constituer une atteinte à la personnalité. L'indication du motif justificatif est par ailleurs abandonnée aux let. b et c, comme cela avait été le cas pour la let. a lors de la révision de 2003[161]. Cette modification vise uniquement à améliorer la clarté; elle correspond à l'art. 28 CC, qui prévoit deux alinéas distincts pour régler d'une part l'atteinte illicite à la personnalité et pour définir d'autre part les motifs justificatifs. Le P-LPD regroupe les motifs justificatifs à l'art. 27.

Al. 3 Absence d'atteinte

Selon l'al. 3, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée expressément au traitement (pour le terme «expressément», se référer au commentaire ci-dessus concernant l'al. 2, let. b). Cette règle est reprise telle quelle du droit en vigueur. Elle est logique puisque, dans un tel cas de figure, la liberté individuelle de disposer de ses données ne peut en principe pas être violée. La formulation «en règle générale» montre bien que l'on exprime une présomption légale et non une fiction. La personne concernée peut ainsi apporter la preuve, dans un cas individuel, qu'il y a malgré tout une atteinte à sa personnalité. Cette possibilité est appropriée et impor-

161 Cf. ATF **136** II 508, consid. 5.2.3.

tante, car la distinction entre sphère privée et domaine public est de plus en plus difficile à faire.

Art. 27 Motifs justificatifs

L'art. 27 définit les motifs justifiant une atteinte à la personnalité. Il correspond à la norme en vigueur sous réserve de quelques modifications de portée mineure.

Al. 1 Principe

L'al. 1 pose le principe selon lequel une atteinte à la personnalité – soit tout traitement de données portant atteinte à la personnalité – est illicite, à moins qu'elle ne soit justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public, ou par la loi. Cette disposition reprend la règle définie à l'art. 28, al. 2, CC. Dans le cas où la personne concernée donne son consentement ou que le motif justificatif est prévu par la loi, il n'y a en principe pas de pesée des intérêts et l'al. 2 ne s'applique pas. Parmi les motifs justificatifs prévus par la loi, on peut citer par exemple l'obligation de traitement et l'obligation de vérification (par ex. les art. 28 ss de la loi fédérale du 23 mars 2001 sur le crédit à la consommation[162] ou les art. 3 ss de la loi fédérale du 10 octobre 1997 sur le blanchiment d'argent[163]) ou l'obligation de conservation. Il y aura en revanche une pesée des intérêts lorsque le motif justificatif réside dans un intérêt privé ou public prépondérant. Du côté de la personne concernée, l'intérêt réside entre autres dans la protection de sa liberté de disposer librement de ses données. Du côté du responsable du traitement, l'intérêt réside dans le traitement des données. L'al. 2 donne une liste exemplative des traitements susceptibles de représenter un intérêt prépondérant du responsable du traitement. L'atteinte à la personnalité ne sera licite que si l'intérêt au traitement des données du responsable du traitement l'emporte sur l'intérêt de la personne concernée.

Al. 2 Intérêts prépondérants du responsable du traitement

L'al. 2 liste les cas dans lesquels les intérêts prépondérants du responsable du traitement entrent en considération. La formulation, qui est restée la même par rapport au droit actuel, montre clairement que les cas énumérés ne constituent pas des motifs justificatifs absolus. Comme dans le droit actuel, le résultat de la pesée des intérêts dans le cas d'espèce est déterminant. Contrairement au droit actuel, on ne parle plus de la personne qui traite des données personnelles, mais du responsable du traitement. La modification est due à l'introduction de la notion de «responsable du traitement». Les motifs justificatifs prévus à l'art. 27 al. 2, s'adressent aux personnes qui, en tant que responsables du traitement, décident des finalités et des moyens du traitement des données. D'autres défendeurs peuvent faire valoir les motifs justificatifs de l'al. 1. En vertu de l'art. 8, al. 4, le sous-traitant peut faire valoir les mêmes motifs justificatifs que le responsable du traitement. La légitimation passive n'est pas affectée par la modification.

162 RS **221.214.1**
163 RS **955.0**

La liste correspond pour l'essentiel à celle qui est en vigueur actuellement. L'énumération n'est pas exhaustive, de sorte que d'autres motifs sont susceptibles de constituer un intérêt prépondérant du responsable du traitement. Elle mentionne diverses finalités qui justifient un traitement des données et qui peuvent l'emporter sur l'intérêt de la personne concernée. Schématiquement, le catalogue comprend trois catégories de traitements de données: ceux réalisés à des fins économiques, ceux réalisés pour le compte des médias et ceux réalisés à des fins ne se rapportant pas à des personnes, telles que la recherche par exemple. Dans certains cas, la finalité du traitement ne suffit pas à elle seule à justifier une atteinte à la personnalité. Le traitement doit respecter certaines conditions supplémentaires afin que le motif justificatif puisse le cas échéant être invoqué. Il s'agit principalement des let. b, c, e et f. Dans ces cas, il faut en premier lieu examiner si le traitement en question respecte les conditions légales avant de procéder à une pesée des intérêts en cause. Si ces conditions spécifiques ne sont pas réalisées, le traitement n'est licite que s'il existe un motif justificatif au sens de l'al. 1. Seules les lettres c et e, qui ont connu des modifications dans le texte de loi, sont commentées ci-dessous.

Let. c Contrôle de la solvabilité

En ce qui concerne l'activité d'entreprises de renseignements de solvabilité, il est tout d'abord important de signaler le récent arrêt du Tribunal administratif fédéral A-4232/2015 du 18 avril 2017 (Moneyhouse). Moneyhouse AG est une entreprise de renseignements de solvabilité qui reçoit des données sous forme électronique de la part de diverses sources publiques et privées. Cette multitude de données personnelles est publiée sur www.moneyhouse.ch et est utilisée pour proposer différents types de services, notamment un moteur de recherche d'entreprises et de personnes. Alors que ce service est gratuit, moyennant enregistrement sur le site, d'autres sont payants, et réservés aux «*Premium Users*»: accès à des informations sur la solvabilité et la moralité de paiement ou encore à des renseignements détaillés sur les défauts de paiement, les actes de poursuite, le registre foncier et la situation économique et fiscale, ainsi que des services relatifs à des portraits d'entreprises. Pour les offres supplémentaires et pour pouvoir accéder aux données des personnes physiques qui ne sont pas inscrites au registre du commerce ou dans un annuaire téléphonique électronique, une pièce justificative prouvant l'intérêt doit être fournie[164]. En ce qui concerne les abonnements payants, le Tribunal administratif fédéral est arrivé à la conclusion que Moneyhouse AG établit un portrait biographique des personnes. Il a estimé que, dans ce contexte, le traitement des données portait sur des profils de personnalité, et qu'en conséquence, le motif justificatif tiré de l'art. 13, al. 2, let. c, LPD, ne pouvait être invoqué[165]. Par ailleurs, pour le Tribunal administratif fédéral, ni une base juridique ni l'accord exprès de la personne concernée ne pouvait justifier la création de profils de personnalité. Une pesée des intérêts en présence a enfin révélé que l'intérêt de la personne concernée à la protection de ses droits de la personnalité l'emportait. Le Tribunal administratif fédéral a estimé que Moneyhouse AG traitait des profils de la personnalité de manière illicite. Il lui a ordonné de demander l'accord exprès des personnes concernées pour ce genre de traitement de

164 TAF, A-4232/2015 du 18 avril 2017, état de fait A.a.
165 TAF, A-4232/2015 du 18 avril 2017, consid. 5.3

données, ou de supprimer les données correspondantes car il est possible d'en déduire des aspects importants de la personnalité[166]. De plus, le tribunal a ordonné à Moneyhouse AG un contrôle annuel de sa base de données en vérifiant 5 % des requêtes soumises sur son site[167]. En outre, le Conseil fédéral va, dans le cadre du rapport sur le postulat Schwaab 16.3682 «Encadrement des pratiques des sociétés de renseignement de solvabilité» examiner des mesures spécifiques pour les sociétés de renseignements commerciaux.

Le P-LPD prend en compte certaines préoccupations liées aux activités des entreprises de renseignements de solvabilité. Ainsi, quatre conditions doivent être remplies pour qu'un contrôle de solvabilité soit considéré comme étant un intérêt prépondérant. La disposition a été légèrement renforcée par rapport au droit actuel, en particulier pour prendre en considération les risques liés à ce genre de traitements.

Les *ch. 1 et 2* correspondent à la teneur actuelle de la loi, à ceci près que la notion de profil de la personnalité a été remplacée par celle de profilage. Le traitement de données sensibles reste aussi interdit. En font partie les données sur les poursuites pénales et sur les sanctions. Cette limitation est cohérente, dans la mesure où des tiers n'ont pas d'accès au casier judiciaire. La LPD, contrairement à l'avis de différents participants à la procédure de consultation externe, ne saurait à cet égard donner davantage de droits aux entreprises de renseignements de solvabilité.

Les *ch. 3 et 4* sont nouveaux.

En vertu du *ch. 3*, les données ne doivent pas dater de plus de cinq ans. Un tel renforcement a été demandé par plusieurs participants à la procédure de consultation externe et paraît justifié, compte tenu des possibles conséquences d'un rapport de solvabilité pour la personne concernée. Le Tribunal administratif fédéral a d'ailleurs jugé que plus les risques d'une atteinte à la personnalité sont grands, plus les exigences relatives à la qualité des données, et donc à l'exactitude des données traitées, doivent être élevées[168]. Le taux de vérification très faible de 5 % imposé à Moneyhouse AG montre en même temps qu'il est très difficile de garder de telles bases de données à jour. Par conséquent, le Conseil fédéral juge opportun d'introduire une règle générale sur la durée pendant laquelle les données peuvent être utilisées. Cette restriction pourra être mise en œuvre notamment par des mesures techniques (*privacy by design*, cf. art. 6 P-LPD et les explications y relatives), telles que l'effacement automatique des données après une certaine période. Le délai de conservation de cinq ans fait écho à l'art. 8*a*, al. 4, LP, selon lequel le droit de consultation des tiers s'éteint cinq ans après la clôture de la procédure. Les droits des entreprises de renseignements de solvabilité ne sauraient aller plus loin.

Le *ch. 4*, prévoit que la personne concernée doit être majeure. Cette condition est introduite pour améliorer la protection des mineurs, ce qui est un des buts de la révision. La portée de cette modification devrait être limitée en raison de la capacité juridique restreinte des personnes mineures.

166 TAF, A-4232/2015 du 18 avril 2017, consid. 5.5
167 TAF, A-4232/2015 du 18 avril 2017, consid. 7.3.2
168 TAF, A-4232/2015 du 18 avril 2017, consid. 7.1.

Let. e Traitement à des fins de recherche, de planification et de statistique

Le motif justificatif prévu à la let. e, pour les traitements de données personnelles à des fins qui ne se rapportent pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, est légèrement renforcé. Ce type de traitement de données n'est dorénavant licite que si les conditions des al. 1 à 3 sont remplies. Cette réglementation doit renforcer la protection des données sensibles. Cette mesure tient compte des possibilités offertes par les mégadonnées et de l'importance toujours plus grande du numérique dans la vie quotidienne, qui implique également une augmentation du nombre de traitements de données sensibles.

En vertu du *ch. 1*, les données personnelles doivent être rendues anonymes dès que le but du traitement le permet. Ainsi, lorsqu'il n'est plus nécessaire de disposer de données personnelles pour la recherche, la planification ou la statistique, ces données doivent être anonymisées. Cette condition est réalisée lorsque les données sont communiquées sous une forme pseudonymisée et que la clé pour réidentifier la personne reste chez celui qui transmet les données (anonymisation factuelle).

Ce principe résulte déjà de l'art. 5, al. 4, P-LPD. Une violation de cette règle constitue une atteinte à la personnalité selon l'art. 26, al. 2, let. a, qui peut être justifiée par un des motifs prévus à l'art. 27. En vertu de la nouvelle disposition prévue à l'art. 27, al. 2, let. e, ch. 1, P-LPD, il n'est dorénavant plus possible de justifier une violation de l'art. 5, al. 4, P-LPD au motif qu'il s'agit d'un traitement à des fins de recherche, de planification ou de statistique.

Des données sensibles ne peuvent être communiquées à des tiers que sous une forme ne permettant pas d'identifier la personne concernée (*ch. 2*). La communication de données sensibles à des tiers constitue une atteinte à la personnalité selon l'art. 26, al. 2, let. c, P-LPD qui peut être justifiée par un des motifs prévus à l'art. 27. En vertu de la nouvelle condition prévue au ch. 2, il n'est dorénavant plus possible de justifier une communication de données personnelles sensibles à des tiers au motif qu'il s'agit d'un traitement à des fins de recherche, de planification ou de statistique.

Enfin, en vertu du *ch. 3*, les résultats ne peuvent être publiés que sous une forme ne permettant pas d'identifier les personnes concernées, comme c'est du reste le cas aujourd'hui.

Art. 28 Prétentions

L'art. 28 définit les prétentions que la personne concernée peut faire valoir contre des personnes privées.

Al. 1 Rectification

L'al. 1 dispose que toute personne peut exiger la rectification de données personnelles inexactes. Cette revendication se trouve jusqu'à présent à l'art. 5, al. 2, LPD. Dans le P-LPD, elle est fusionnée avec toutes les autres prétentions juridiques dans une seule disposition. La rectification peut signifier soit que les données manquantes sont ajoutées, soit que les données erronées sont détruites et, le cas échéant, remplacées par de nouvelles données correctes.

Cet alinéa fait ressortir clairement que le droit à la rectification est indépendant d'une atteinte à la personnalité au sens de l'art. 26 P-LPD. Les motifs justificatifs de l'art. 27 P-LPD ne peuvent pas être invoqués non plus. L'al. 1 prévoit toutefois deux exceptions qui excluent une rectification.

Selon la *let. a*, la demande de rectification des données n'est pas possible si la modification est interdite par une prescription légale. On pense ici aux obligations légales de traitement ou de conservation des données en vertu desquelles des données personnelles privées ne doivent pas être modifiées.

La *let. b* autorise une pesée des intérêts en ce qui concerne les données traitées uniquement à des fins archivistiques et qui répondent à un intérêt public prépondérant voulant que les données restent inchangées. Cette exception couvre, par exemple, les bibliothèques privées.

Al. 2 Actions en justice

Cette disposition renvoie aux actions régies par les art. 28 ss CC en vigueur. A l'instar de l'art. 28*a*, al. 1, CC, l'al. 2 détermine les prétentions spécifiques que la personne concernée peut faire valoir. Par souci de clarté, le P-LPD énumère ces prétentions. Cette énumération concrétise notamment l'action visant à interdire et à faire cesser l'atteinte illicite au sens de l'art. 28*a*, al. 1, ch. 1 et 2, CC en matière de protection des données. En vertu de la *let. a*, la personne concernée peut exiger l'interdiction du traitement de données personnelles. Conformément à la *let. b*, elle peut également demander l'interdiction de la communication des données à des tiers. Enfin, elle peut exiger l'effacement ou la destruction des données (*let. c*).

Bien que le droit en vigueur prévoie déjà implicitement un droit à l'effacement des données, le projet propose de le prévoir expressément. Cela correspond aux exigences de l'art. 8, let. e, P-STE 108. L'art. 17 du règlement (UE) 2016/679 contient une disposition similaire. Le droit à l'effacement correspond dans le domaine de la protection des données au «droit à l'oubli», tel que conféré de manière générale par la protection de la personnalité du droit civil[169]. Une décision analogue à celle rendue par la Cour de justice européenne[170] contre Google serait donc également possible en Suisse. Le droit à l'oubli n'est toutefois pas absolu[171]. La jurisprudence sur la protection des données procède plutôt à une pesée des intérêts en cause, à savoir, d'une part, l'intérêt de la personne concernée et, d'autre part, la liberté d'opinion ou d'information dont résulte souvent un intérêt au maintien et à l'utilisation de l'information. Un tel intérêt peut résulter par exemple des archives ou des bibliothèques qui ont pour tâches de collecter des documents sans qu'ils soient modifiés, de les mettre en valeur, de les obtenir et de les faire connaître.

La pesée des intérêts à faire dans un cas particulier étant possible et nécessaire sur la base de l'art. 28, al. 2, P-LPD ainsi que du renvoi aux actions des art. 28 s. CC,

169 Cf. ATF **109** II 353, **111** II 209 et **122** III 449.
170 Voir le jugement de la CJUE. C-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González) du 13 mai 2014, ECLI:EU:C:2014:317.
171 ATF **111** II 209, consid. 3c

aucune clause spécifique n'a dû être incluse dans le texte de loi[172]. Le préposé aurait souhaité que l'on introduise expressément un «droit au déréférencement» (droit à l'oubli numérique).

Al. 3 Mention du caractère litigieux

L'al. 3 reprend du droit en vigueur la mention du caractère litigieux d'une donnée personnelle. Ainsi, lorsque ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie, le demandeur peut requérir que l'on ajoute à la donnée la mention de son caractère litigieux. Cette disposition se comprend en tenant compte du fait que des allégations factuelles inexactes, surtout quand elles sont liées à des jugements de valeur, ne constituent pas une preuve suffisante. De cette manière, la personne concernée peut obtenir une protection juridique partielle.

Al. 4 Communication à des tiers ou publication

L'al. 4 prévoit, comme c'est déjà le cas aujourd'hui, que la rectification, l'effacement ou la destruction des données, l'interdiction du traitement ou de la communication à des tiers notamment, la mention du caractère litigieux ou le jugement soient communiqués à des tiers ou publiés. Cette disposition concrétise l'art. 28*a*, al. 2, CC dans le domaine de la protection des données.

On abroge en revanche la disposition déclarative relative aux actions en exécution du droit d'accès selon la procédure simplifiée. Cette règle est devenue obsolète depuis l'entrée en vigueur du CPC, car toutes les dispositions liées aux procédures civiles y sont maintenant incluses (art. 12, al. 4, CPC). Ce texte règle la procédure applicable (art. 243, al. 2, let. d, P-CPC) ainsi que le for juridique (art. 20, let. d, P-CPC).

9.1.7 Dispositions particulières pour le traitement de données personnelles par des organes fédéraux

Art. 29 Contrôle et responsabilité en cas de traitements de données personnelles conjoints

Par rapport à l'art. 16 LPD, l'art. 29 P-LPD subit quelques modifications.

L'art. 16, al. 1, LPD est supprimé. La responsabilité de l'organe fédéral qui traite ou fait traiter des données personnelles découle de la définition de la notion de «responsable du traitement» (art. 4, let. i, P-LPD).

L'art. 29 P-LPD supprime en outre les termes «de manière spécifique» de l'art. 16, al. 2, pour des motifs rédactionnels. Il prévoit par ailleurs une obligation pour le Conseil fédéral – et non plus seulement une faculté – de régler les procédures de contrôle et les responsabilités en matière de protection des données lorsqu'un organe fédéral traite des données conjointement avec d'autres autorités ou des personnes privées. Cette modification met en œuvre l'art. 21 de la directive (UE) 2016/680. L'art. 26 du règlement (UE) 2016/679 prévoit une réglementation analogue.

172 L'art. 38 ne prévoit pas une telle pesée des intérêts, raison pour laquelle une réserve a été introduite à son al. 5.

Art. 30 Bases légales

Pour donner suite aux critiques de la doctrine par rapport à l'articulation entre les exceptions prévues à l'art. 17, al. 2, LPD et celles énumérées à l'art. 19, al. 2, LPD, le P-LPD prévoit de régler le niveau de la base légale pour certains traitements de données (art. 30, al. 2) et d'autre part d'énumérer les exceptions relatives à l'exigence d'une base légale (art. 30, al. 4).

Al. 1 Base légale

Cette disposition reprend le principe qui figure à l'actuel art. 17, al. 1, LPD, selon lequel les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale, sous réserve de certaines exceptions.

Al. 2 Base légale dans une loi au sens formel

Comme c'est le cas aujourd'hui, l'al. 2, *let. a* prescrit que les traitements de données sensibles doivent reposer sur une base légale au sens formel.

En vertu de l'al. 2, *let. b*, les organes fédéraux ne sont en droit d'effectuer des profilages au sens de l'art. 4, *let. f,* P-LPD que si une base légale au sens formel le prévoit. Cette disposition remplace l'art. 17, al. 2, LPD qui prescrit que des profils de la personnalité ne peuvent être traités que si cela est prévu par une base légale au sens formel. En raison du risque d'atteinte aux droits fondamentaux des personnes concernées, le Conseil fédéral considère que l'exigence du niveau de la base légale pour le profilage doit être la même que celle pour le traitement de données sensibles. Comme on le verra à l'al. 3, l'exigence d'une base légale au sens formel pour ce type de traitements n'est toutefois pas absolue. Il incombera donc au législateur de déterminer dans chaque domaine s'il y a lieu d'adopter une base légale au sens formel dans une loi sectorielle ou si une base légale au sens matériel suffit. Dans certaines situations, on peut envisager qu'un profilage n'implique pas de risques particuliers pour les droits fondamentaux de la personne concernée.

L'al. 2, *let. c* prescrit qu'une base légale au sens formel est exigée lorsque la finalité ou le mode du traitement est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée. Ce cas de figure n'est pas expressément prévu à l'art. 17, al. 2, LPD mais ne constitue pas en soi une exigence nouvelle puisque l'art. 36, al. 1, Cst. prescrit que toute restriction grave d'un droit fondamental doit être fondée sur une base légale prévue par une loi au sens formel. La *let. c* est néanmoins nécessaire en raison de l'abrogation de la notion de «profil de la personnalité» et des bases légales y relatives prévues dans plusieurs lois fédérales. Le Conseil fédéral considère en effet que l'abrogation de la notion de «profil de la personnalité» ne doit pas entraîner une diminution des exigences du niveau de la base légale.

Une atteinte grave aux droits fondamentaux de la personne concernée peut résulter de la finalité du traitement des données personnelles (premier cas d'application de la let. c). Dans certains domaines, les organes fédéraux peuvent en effet être amenés à traiter certaines données personnelles afin d'évaluer par exemple la dangerosité d'une personne, son potentiel à exercer une fonction, son aptitude à accomplir une obligation légale ou encore son mode de vie. En fonction de la finalité poursuivie par

l'organe fédéral, le traitement peut porter gravement atteinte aux droits fondamentaux de la personne concernée, ceci indépendamment de la nature des données traitées. Si tel est le cas, il est justifié que le traitement repose sur une base légale de même niveau que celui pour les traitements de données sensibles.

Une atteinte grave aux droits fondamentaux de la personne concernée peut également résulter du mode de traitement des données personnelles (second cas d'application de la *let. c*). Tel peut être le cas des décisions individuelles automatisées au sens de l'art. 19, al. 1, P-LPD. Certes, toutes les décisions individuelles automatisées ne présentent pas un risque élevé pour les droits des personnes concernées. Le cas échéant, une base légale au sens matériel est suffisante. En principe, lorsque la décision individuelle automatisée se fonde sur un traitement de données sensibles, une base légale au sens formel doit être prévue. Les exigences de l'art. 11 de la directive (UE) 2016/680 sont ainsi respectées.

Al. 3 Exceptions à l'exigence d'une base légale au sens formel

Cette disposition habilite le Conseil fédéral à adopter une base légale au sens matériel pour les traitements de données sensibles et le profilage si deux conditions cumulatives sont remplies. La première (*let. a*) prescrit que le traitement doit être indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel. Pour que cette condition soit réalisée, il faut que le législateur concrétise de manière précise au niveau de la loi la nature des tâches qui nécessiteront des traitements de données personnelles. La seconde condition (al. 3, *let. b*) est nouvelle. Elle présente l'avantage de limiter de manière plus précise la portée de l'al. 3, que ne le fait l'art. 17, al. 2, *let. a*, LPD. En effet, cette disposition ne s'applique qu'à titre exceptionnel, ce qui laisse toujours une marge d'interprétation pour déterminer les cas exceptionnels de ceux qui ne le sont pas.

L'assouplissement du niveau de la base légale est opportun en particulier pour les données sensibles traitées exceptionnellement dans les affaires du Conseil fédéral, des départements et des offices (par exemple, recours, responsabilité de l'Etat, affaires concernant le personnel de la Confédération). Si l'on applique strictement l'art. 17, al. 1, LPD, ce type de traitements doit également reposer sur une base légale au sens formel. En vertu de l'art. 30, al. 3, P-LPD, une base légale au sens matériel sera suffisante, pour autant que le traitement soit indispensable à l'accomplissement d'une tâche définie dans une loi au sens formel et que la finalité du traitement ne présente pas de risques particuliers pour les droits fondamentaux de la personne concernée. Si ces conditions sont remplies et si l'accès à ces données est fortement limité, une base légale au sens matériel est en principe suffisante.

Al. 4 Dérogations

Cette disposition prévoit une dérogation à l'exigence d'une base légale (al. 1 à 3) si l'une des conditions prévues aux let. a à c est réalisée.

La *let. a* vise une décision du Conseil fédéral autorisant exceptionnellement un organe fédéral à traiter des données personnelles sans base légale. Elle correspond à l'exception prévue à l'art. 17, al. 2, let. b, LPD.

En vertu de la *let. b*, les organes fédéraux peuvent également traiter des données si la personne concernée a, en l'espèce, donné son consentement au sens de l'art. 5, al. 6, P-LPD ou si elle a rendu ses données personnelles accessibles à tout un chacun et ne s'est pas opposée expressément au traitement. Cette disposition correspond en substance à l'exception prévue à l'art. 17, al. 2, let. c, LPD.

Enfin, la *let. c* constitue une nouvelle exception qui n'est pas prévue à l'art. 17, al. 2, LPD. Elle correspond à l'art. 10, let. b, de la directive (UE) 2016/680 et à l'art. 6, par. 1, let. d, du règlement (UE) 2016/679. En vertu de cette disposition, les organes fédéraux peuvent traiter des données personnelles si le traitement est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers et s'il n'est pas possible d'obtenir le consentement de la personne concernée dans un délai raisonnable.

Art. 31 Traitement de données personnelles automatisé dans le cadre d'essais pilotes

Les modifications apportées à l'art. 17*a* LPD n'ont pas pour but d'affaiblir les conditions applicables lorsqu'un organe fédéral envisage d'effectuer un traitement de données automatisé dans le cadre d'un essai pilote avant l'entrée en vigueur d'une loi au sens formel, mais uniquement de diminuer la densité normative. En effet, les organes fédéraux ont peu recouru à cette norme depuis son entrée en vigueur. De plus, certaines dispositions de l'art. 17*a* LPD peuvent être fixées dans la future ordonnance d'exécution.

Les conditions fixées aux *al. 1* et *2* sont en substance identiques à celles de l'art. 17*a*, al. 1, LPD, sous réserve que la notion de «profils de la personnalité» est remplacée par celle «d'autres traitements au sens de l'art. 30, al. 2, let. b et c». De plus, il est précisé à la *let. c* qu'une phase d'essai doit être nécessaire, «en particulier pour des raisons techniques». Cette modification est due à la suppression l'art. 17*a*, al. 2, LPD qui énumère dans quels cas une phase d'essai peut être considérée comme indispensable pour traiter des données. Pour les motifs indiqués ci-dessus, ces cas peuvent être réglés dans une ordonnance d'exécution.

Les *al. 3* et *4* sont inchangés par rapport au droit en vigueur, sous réserve de l'abrogation de la notion de «profils de la personnalité» et de certaines modifications rédactionnelles.

Art. 32 Communication de données personnelles

L'art. 32 P-LPD ne modifie pas le principe fixé à l'art. 19 LPD selon lequel les organes fédéraux ne sont, en principe, en droit de communiquer des données personnelles que s'il existe une base légale, mais précise que la notion de base légale correspond à celle prévue à l'art. 30, al. 1 à 3, P-LPD. Il résulte de cette précision que l'art. 32 ne renvoie pas aux exceptions prévues à l'art. 30, al. 4. En effet, les cas dans lesquels les organes fédéraux sont habilités à communiquer des données personnelles, en l'absence d'une base légale, sont énumérés de manière exhaustive à l'art. 32, al. 2, let. a à e, P-LPD. Cette modification tient compte des critiques de la doctrine concernant l'articulation entre les exceptions prévues à l'art. 17, al. 2, LPD et celles énumérées à l'art. 19, al. 2, LPD.

La notion de «données personnelles» de l'*al. 1* vise également les données sensibles. Si l'art. 30 exige une base légale prévue dans une loi au sens formel pour le traitement d'une certaine catégorie de données personnelles (données sensibles) ou pour certains traitements (traitements au sens de l'art. 30, al. 2, *let. b et c*), il en va de même s'agissant des prescriptions relatives à la communication des données en question. La communication de données personnelles est une opération particulièrement sensible en soi, si bien que la manière dont les données communiquées ont été obtenues peut ne pas être anodine. Par conséquent, si des données sont communiquées à la suite d'un traitement particulièrement délicat, la communication doit être prévue dans une loi au sens formel. Les exceptions prévues à l'al. 2*,* sont également applicables lorsqu'un organe fédéral envisage de communiquer ce type de données.

L'exception prévue à l'al. 2, *let. a*, est élargie: en l'absence d'une base légale, un organe fédéral est en droit de communiquer des données dans un cas d'espèce non seulement lorsque ces données sont indispensables au destinataire pour l'accomplissement d'une tâche légale mais aussi lorsque cela est indispensable pour l'organe fédéral qui envisage de communiquer les données.

La *let. c* constitue une nouvelle exception qui n'est pas prévue à l'art. 19, al. 1, LPD. Elle est également introduite à l'art. 30, al. 4, let. c, P-LPD.

L'*al. 3* correspond à l'art. 19, al. 1bis, LPD, sous réserve d'une modification ponctuelle. Cette adaptation a pour but d'améliorer la coordination entre la LTrans et la LPD en indiquant clairement que la condition prévue à la *let. b* (existence d'un intérêt public prépondérant) constitue non seulement une alternative par rapport aux al. 1 et 2, mais qu'elle est également indépendante de ces dispositions. La mesure proposée consiste à remplacer, dans la phrase introductive de l'al. 3, le terme «*auch*» (qui n'existe pas dans la version française) par celui de «*darüber hinaus* / en outre» afin de montrer explicitement que l'al. 3 constitue une base légale supplémentaire à celles prévues aux al. 1 et 2.

L'*al. 4*, ne subit pas de modification par rapport à l'art. 19, al. 2, LPD. Les explications du message du Conseil fédéral du 23 mars 1988[173] restent valables.

Par contre, l'exigence de base légale pour les «procédures d'appel» dans le secteur public est abandonnée (art. 19, al. 3, LPD), car elle est dépassée à l'ère de la société numérique. Cette modification n'a pas pour conséquence d'affaiblir la protection des données personnelles, puisqu'il s'agit toujours d'une communication qui doit respecter les conditions légales de protection des données. Les modifications de lois sectorielles qui découlent de l'abrogation de l'art. 19, al. 3, LPD devront être faites au fur et à mesure des révisions de ces lois.

Les *al. 5 et 6* correspondent aux al. 3bis et 4 de l'art. 19 LPD.

Art. 33 Opposition à la communication de données personnelles

Cette disposition correspond à l'art. 20 LPD, sous réserve de certaines modifications rédactionnelles. Dans la version allemande, les termes «*Sperrung der Bekanntgabe*»

173 FF **1988** 477

sont remplacés par l'expression «*Widerspruch gegen die Bekanntgabe*» pour mieux s'aligner sur la terminologie européenne.

De l'avis du préposé, le droit d'opposition ne devrait pas se limiter à la communication, mais devrait porter aussi sur les traitements de données.

Art. 34 Proposition des documents aux Archives fédérales

Cette disposition correspond à l'art. 21 LPD. Elle ne subit pas de modifications matérielles.

Art. 35 Traitements à des fins de recherche, de planification et de statistique

Cette disposition correspond pour l'essentiel à l'art. 22 LPD.

Le nouvel *al. 1*, *let. b*, précise que l'organe fédéral ne communique des données sensibles que sous une forme ne permettant pas d'identifier les personnes concernées. Cette modification vise à renforcer la protection des données sensibles. Cette condition est réalisée lorsque les données sont communiquées sous une forme pseudonymisée, et que la clé pour réidentifier la personne reste chez celui qui transmet les données (anonymisation factuelle).

Deux modifications sont en outre apportées à l'*al. 2*, concernant les renvois aux art. 5, al. 3, 30, al. 2, et 32, al. 1, P-LPD.

Art. 36 Activités de droit privé exercées par des organes fédéraux

Cette disposition correspond à l'art. 23, al. 1, LPD. L'al. 2 de l'art. 23 LPD peut être supprimé puisque le P-LPD prévoit le même système de surveillance pour les personnes privées et les organes fédéraux.

Art. 37 Prétentions et procédure

Par rapport à l'art. 25 LPD, l'art. 37 subit certaines modifications qui sont présentées ci-dessous.

Al. 1 Prétentions

Cette disposition règle les prétentions que les personnes concernées peuvent faire valoir contre des organes fédéraux. Elle ne subit pas de modification par rapport à l'art. 25, al. 1, LPD.

Al. 2 Autres prétentions

Aujourd'hui, le droit pour la personne concernée d'exiger l'effacement de ses données découle implicitement de l'art. 25 LPD. Pour mettre en œuvre les exigences de l'art. 8, let. e, P-STE 108 et de l'art. 16 de la directive (UE) 2016/680, ce droit est maintenant expressément fixé à l'art. 37, al. 2, let. a et b, P-LPD. L'art. 17 du règlement (UE) 2016/679 prévoit quant à lui un droit pour la personne concernée d'exiger, à certaines conditions, l'effacement de ses données («droit à l'oubli»). L'art. 28 P-LPD prévoit le même droit, de sorte que la réglementation est iden-

tique pour les responsables du traitement des secteurs privé et public (ch. 9.1.6). Cette modification ne comporte néanmoins pas de changement par rapport à la situation légale.

Par rapport à l'art. 25, al. 3, let. a, LPD, le nouvel al. 2, *let. a*, est modifié en ce sens que la dernière partie de la phrase concernant l'opposition à la communication à des tiers est supprimée. En effet ce droit est expressément régi par l'art. 33 P-LPD[174]. Le droit de s'opposer à la communication de données personnelles en vertu de l'art. 33 n'est pas lié à un traitement illicite, contrairement aux prétentions prévues à l'art. 37.

La *let. b* prévoit que la personne concernée peut demander que l'organe fédéral publie sa décision concernant son opposition à une communication de données personnelles selon l'art. 33. L'art. 33 ne prévoit pas une telle possibilité. Il est judicieux que la personne concernée puisse au moins exiger cette publication lorsque la communication de données personnelles est illicite.

Al. 3 Limitation du traitement

L'al. 3 prévoit une mesure moins radicale que l'effacement ou la destruction des données personnelles litigieuses, à savoir la limitation du traitement.

Cette réglementation correspond à l'art. 16, par. 3, de la directive (UE) 2016/680, qui prévoit qu'au lieu de procéder à l'effacement des données litigieuses, le responsable du traitement limite le traitement lorsque l'exactitude des données est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non, ou lorsque les données doivent être conservées à des fins probatoires.

L'art. 18 du règlement (UE) 2016/679 va plus loin, puisqu'il prévoit un droit pour la personne concernée d'exiger la limitation du traitement.

La limitation du traitement n'est en revanche par prévue par le P-STE 108.

L'al. 3 doit être interprété dans ce sens que le traitement reste possible, mais uniquement s'il poursuit certaines finalités. En effet, il ne s'agit pas d'exclure tout type de traitement. Comme il ressort du considérant 47 de la directive (UE) 2016/680, la limitation d'un traitement doit être comprise en ce sens que l'organe fédéral ne peut traiter les données concernées que pour les finalités qui ont empêché leur effacement. L'al. 3 prévoit quatre cas de figure.

Selon la *let. a*, l'organe fédéral doit limiter le traitement des données lorsque leur exactitude est contestée par la personne concernée et que leur exactitude ou inexactitude ne peut pas être établie. Dans ce cas de figure, la limitation du traitement signifie que l'organe fédéral ne peut traiter les données litigieuses que dans le but de constater leur exactitude ou leur inexactitude. Une fois l'exactitude des données établie, l'organe fédéral peut poursuivre le traitement sans autres restrictions. Si par contre les données personnelles s'avèrent inexactes, l'organe fédéral doit les effacer ou les détruire, à moins que les let. b ou c ne s'appliquent au cas d'espèce.

174 Voir à ce sujet Bangert Jan, commentaire des art. 25 et 25bis LPD, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3e édition, Bâle 2014, ch. 62 ss.

La *let. b* prescrit que l'organe fédéral doit limiter le traitement lorsque la protection d'intérêts prépondérants d'un tiers l'exige, par exemple lorsque l'effacement ou la destruction de certaines données pourrait empêcher une tierce-personne d'exercer ses droits en justice. Cette mesure signifie que le traitement des données ne reste possible que s'il a pour but de permettre au tiers concerné d'exercer ses droits. Tout traitement poursuivant une autre finalité est exclu.

En vertu de la *let. c*, l'organe fédéral n'est pas tenu d'effacer ou de détruire des données litigieuses lorsqu'une telle mesure risque de porter atteinte à un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Suisse.

Enfin, la *let. d* dispose que l'organe fédéral n'est pas non plus tenu d'effacer ou de détruire des données lorsqu'une telle mesure risque de compromettre une enquête, une instruction ou une procédure judiciaire ou administrative. Dans ce cas de figure, l'organe fédéral peut continuer à traiter des données personnelles, mais uniquement pour les finalités qui ont empêché leur effacement, à savoir la poursuite d'une enquête, d'une instruction ou d'une procédure.

La limitation du traitement signifie que les données litigieuses doivent être marquées de telle manière qu'elles ne puissent être traitées que pour la finalité qui a empêché leur effacement ou leur destruction. Le marquage doit être clair. Une solution envisageable en pratique est de faire migrer provisoirement les données litigieuses dans un autre système. Il est également possible de bloquer les droits d'accès des utilisateurs. Dans des systèmes de traitement automatisé de données, la limitation du traitement devrait être garantie par des mesures techniques, de manière à empêcher tout traitement ultérieur ou modification des données pour des finalités autres que celles définies à l'al. 3.

Al. 4 Mention du caractère litigieux

Cette disposition prévoit la mention du caractère litigieux d'une donnée, mesure qui a été reprise du droit en vigueur (art. 25, al. 2, LPD). Lorsque l'exactitude ou l'inexactitude d'une donnée ne peut définitivement pas être établie, l'organe fédéral doit ajouter la mention de son caractère litigieux.

Al. 5 Fonds d'institutions patrimoniales publiques

Cette disposition prescrit que la rectification, l'effacement ou la destruction de données ne peut être exigée des institutions ouvertes au public, telles que des bibliothèques, des établissements d'enseignement, des musées, des archives ou d'autres institutions patrimoniales publiques, pour les fonds qu'elles gèrent. L'exception a une portée limitée dans la mesure où beaucoup de ces institutions sont régies par le droit cantonal. Cette disposition vise des institutions publiques qui ont notamment comme activité de collecter des documents en tout genre (y compris sous forme numérique) de les exploiter et de les rendre accessibles. Une rectification, un effacement ou une destruction de données personnelles irait à l'encontre d'une telle finalité, pour autant que cette mesure se réfère aux fonds archivistiques de ces institutions. La mention du caractère litigieux ne s'applique pas non plus. En effet, ces fonds doivent, au moyen de documents, représenter un moment du passé, ce qui n'est possible que si ces documents sont conservés dans les archives dans leur forme

originale et donc sans subir de modifications. Il en va d'un intérêt public prépondérant qui résulte de la liberté d'information (art. 16, al. 3, Cst.).

La *seconde phrase* de l'al. 5 confère néanmoins le droit pour la personne concernée d'exiger de l'institution concernée qu'elle limite l'accès aux données litigieuses. La personne concernée doit dans ce cas rendre vraisemblable qu'elle dispose d'un intérêt prépondérant. Cette exception doit être considérée au regard de la tendance toujours plus grande de rendre accessibles les fonds d'institutions patrimoniales publiques sur Internet. Cette pratique permet de réduire le temps de travail nécessaire pour des recherches ciblées, mais élargit en même temps considérablement le cercle des personnes susceptibles d'avoir accès aux documents en question. Pour de tels cas, la loi doit dès lors permettre une pesée des intérêts en cause. Il s'agit d'une part de l'intérêt public à un accès illimité et complet aux documents et d'autre part de l'intérêt de la personne concernée à ne pas rendre accessibles à tout un chacun des informations fausses ou constituant des atteintes à sa personnalité. Il résulte de la première phrase de l'al. 5 que l'intérêt public à un accès illimité et complet prévaut en principe en ce qui concerne les archives et autres institutions analogues. Les intérêts de la personne concernée ne doivent prévaloir que si l'accès libre aux documents engendre d'importants inconvénients pour elle, qui peuvent également constituer une entrave considérable dans sa vie future (par ex. dans sa carrière professionnelle). Ces inconvénients doivent également être mis en relation avec la valeur archivistique des données litigieuses, qui peut résulter par exemple de l'importance historique, du type ou du contenu du document. L'intérêt de la personne concernée doit être considéré comme prépondérant par exemple lorsque la valeur archivistique des données, et donc l'importance d'un accès public illimité, est faible par rapport aux importants inconvénients causés à la personne concernée. Dans une telle hypothèse, la personne concernée peut exiger que l'institution limite l'accès aux données litigieuses. Dans le cas d'espèce, la limitation doit être prévue de telle manière qu'elle respecte le principe de proportionnalité au regard des intérêts en jeu. Par exemple, il peut souvent suffire de ne pas rendre un document accessible sur Internet mais uniquement sous une forme matérielle auprès des archives. Dans certains cas, il est également envisageable d'accorder l'accès uniquement à certaines personnes, qui ont en besoin pour leurs activités scientifiques ou archivistiques.

Ne tombent pas sous l'al. 5 en revanche les traitements de ces institutions qui ne sont pas en rapport avec leurs fonds, ou qui poursuivent d'autres buts, comme par exemple les comptes d'utilisateurs des bibliothèques ou les dossiers personnels. Pour ces traitements, la personne concernée dispose de toutes les prétentions de l'art. 37 P-LPD.

Art. 38 Procédure en cas de communication de documents officiels contenant des données personnelles

Cette disposition correspond à l'art. 25bis LPD. Elle ne subit pas de modifications matérielles.

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

9.1.8.1 Organisation

Art. 39 Nomination et statut

Al. 1 Procédure de nomination

La procédure de nomination du préposé régie à l'al. 1 reste inchangée. Elle est conforme aux exigences de la directive (UE) 2016/680 et du P-STE 108. Le P-STE 108 ne prévoit pas de disposition concernant le mode d'élection ou de nomination de l'autorité de contrôle. L'art. 43 de la directive (UE) 2016/680 oblige quant à lui les Etats Schengen à régler la procédure de nomination, tout en leur laissant le choix entre une nomination par le parlement, le gouvernement, le chef d'Etat ou encore par un organisme indépendant. L'art. 53 du règlement (UE) 2016/679 prévoit la même solution pour les Etats membres de l'Union européenne.

Le Conseil fédéral a examiné la proposition de plusieurs participants à la procédure de consultation externe de prévoir une élection du préposé par le Parlement. Il est arrivé à la conclusion qu'il n'est pas opportun de procéder à une telle modification pour les raisons suivantes. La procédure actuelle offre des garanties suffisantes par rapport à l'indépendance du préposé face à l'exécutif. En effet, l'Assemblée fédérale peut refuser d'approuver la nomination du Conseil fédéral. Le Conseil fédéral n'est pas non plus convaincu qu'une élection par le Parlement renforcerait l'indépendance du préposé. Son élection pourrait en effet être influencée par des groupes d'intérêts. Par ailleurs, la nomination du préposé par le Conseil fédéral sous réserve de l'approbation du Parlement permet de maintenir le rattachement administratif du préposé à la Chancellerie fédérale, ce qui ne serait plus possible si celui-ci devait être élu par le Parlement. Si le préposé ne devait plus faire partie de l'administration fédérale, il n'est pas exclu qu'il soit plus difficile pour lui d'exercer ses tâches de surveillance à l'égard des organes fédéraux et d'obtenir leur collaboration lors d'une enquête. Enfin, le corollaire d'une élection du préposé par le Parlement devrait être l'octroi d'une indépendance budgétaire, comme c'est le cas par exemple pour le Contrôle fédéral des finances.

Al. 3 Statut

L'al. 3, *1re phrase*, concrétise l'indépendance du préposé en précisant qu'il ne doit recevoir ni solliciter d'instructions de la part d'une autorité ou d'un tiers. Cette modification tient compte des exigences de l'art. 12bis, par. 4, P-STE 108 et de l'art. 42, par. 1 et 2, de la directive (UE) 2016/680, qui a la même teneur que l'art. 52, par. 1 et 2, du règlement (UE) 2016/679.

Al. 2, 4 et 5

Ces dispositions ne subissent aucune modification matérielle par rapport au droit en vigueur (art. 26, al. 2, 4 et 5, LPD). Le préposé estime que son budget devrait être soumis au même régime que celui du Contrôle fédéral des finances.

Art. 40 Renouvellement et fin des rapports de fonction

Actuellement, la période de fonction du préposé peut être reconduite un nombre indéterminé de fois. Ce principe est modifié afin de transposer les exigences de l'art. 44, par. 1, let. e, de la directive (UE) 2016/680, qui prévoit que les Etats Schengen doivent régler le caractère renouvelable ou non renouvelable du mandat du ou des membres de chaque autorité de contrôle et, si c'est le cas, le nombre de mandats. Cette disposition laisse donc le choix aux Etats Schengen de décider si l'autorité de contrôle peut être reconduite ou non dans ses fonctions et, si oui, le nombre de fois. A noter que l'art. 54, par. 1, let. e, du règlement (UE) 2016/679 prévoit une règle similaire.

Conformément à la marge de manœuvre conférée par l'art. 44 de la directive (UE) 2016/680, le Conseil fédéral propose que le préposé puisse être reconduit dans ses fonctions deux fois. Ce dernier peut donc rester en fonction pendant douze ans au maximum. Cette mesure permet de renforcer l'indépendance du préposé en tant qu'autorité. La crainte pour le préposé de ne pas être reconduit dans sa fonction ne doit pas constituer un frein à l'accomplissement de ses tâches légales. Si le préposé atteint l'âge de la retraite pendant son mandat, les rapports de travail s'éteignent automatiquement à l'âge fixé à l'art. 21 de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[175] (art. 10, al. 1, de la loi du 24 mars 2000 sur le personnel de la Confédération (LPers)[176], par renvoi de l'art. 14, al. 1, LPers).

Les *al. 2, 3 et 4* ne subissent pas de modifications matérielles par rapport à l'art. 26*a* LPD.

Art. 41 Activité accessoire

L'art. 41 renforce les conditions applicables à l'exercice d'une activité accessoire par le préposé. Cette disposition met en œuvre les exigences de l'art. 42, par. 3, de la directive (UE) 2016/680, qui a la même teneur que l'art. 52, par. 3, du règlement (UE) 2016/679. Elle ne s'applique qu'au préposé. Son suppléant et son secrétariat sont soumis aux dispositions de la LPers.

Alors que l'art. 26*b* LPD se limite à prévoir que le Conseil fédéral peut autoriser le préposé à exercer une autre activité pour autant que son indépendance et sa réputation n'en soient pas affectées, l'*al. 1*, *1re phrase*, pose le principe selon lequel le préposé ne peut exercer aucune autre activité rémunérée. La *2e phrase* précise que celui-ci ne peut pas non plus exercer une fonction au service de la Confédération ou d'un canton. La notion de «canton» doit être comprise dans un sens large, à savoir qu'elle vise également les communes, districts, cercles et corporations de droit public. La seconde phrase prescrit en outre que le préposé ne peut pas non plus être membre de la direction, du conseil d'administration, de l'organe de surveillance ou de l'organe de révision d'une entreprise commerciale, ceci indépendamment de la question de savoir si son activité est rémunérée ou non.

175 RS **831.10**
176 RS **172.220.1**

L'*al. 2* limite la portée de l'al. 1. Il prévoit que le Conseil fédéral peut autoriser le préposé à exercer une activité accessoire à certaines conditions. La décision du Conseil fédéral est publiée.

Art. 42 Autocontrôle du préposé

Cette disposition oblige le préposé à s'assurer par des mesures de contrôle appropriées, qui porteront notamment sur la sécurité des données personnelles, du respect et de la bonne application des dispositions fédérales de protection des données en son sein. Le Conseil fédéral concrétisera dans la future ordonnance les mesures à prendre.

9.1.8.2 Enquêtes concernant des violations des prescriptions de protection des données

Art. 43 Enquête

Le droit en vigueur prévoit une procédure différente selon que le préposé exerce ses tâches de surveillance à l'égard du secteur privé ou du secteur public. Tandis que l'art. 27 LPD prescrit que le préposé est chargé de surveiller les traitements de données effectués par les organes fédéraux, les let. a à c de l'art. 29, al. 1, LPD disposent respectivement que ladite autorité ouvre une enquête à l'encontre d'une personne privée lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes, lorsque des fichiers doivent être enregistrés en vertu de l'art. 11*a* LPD ou lorsqu'il existe un devoir d'information en vertu de l'art. 6, al. 3, LPD. L'étendue du pouvoir de surveillance du préposé à l'égard du secteur privé n'est actuellement pas conforme aux exigences du P-STE 108. En effet, l'art. 12bis ne limite pas les cas dans lesquels l'autorité de contrôle peut exercer ses pouvoirs d'investigation et d'intervention auprès d'un responsable du traitement.

Al. 1 Ouverture de l'enquête

En vertu de l'art. 43, al. 1, le préposé est tenu d'ouvrir une enquête d'office ou sur dénonciation dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données. Le dénonciateur peut être un tiers ou la personne concernée. Il n'a toutefois pas qualité de partie à la procédure (cf. art. 46, al. 2, a contrario). Par contre, si c'est la personne concernée qui est l'auteur de la dénonciation, le préposé est tenu de l'informer de la suite donnée à sa dénonciation (al. 4). Pour faire valoir ses droits, la personne concernée doit agir selon les voies de droit applicables, à savoir par voie civile si le responsable du traitement est une personne privée ou par voie de recours contre la décision rendue par l'organe fédéral responsable, comme c'est du reste le cas aujourd'hui.

Al. 2 Renonciation à l'ouverture d'une enquête

Le préposé peut renoncer à ouvrir une enquête lorsque la violation des prescriptions de protection des données est de peu d'importance. Tel serait le cas par exemple si une association sportive ou culturelle a envoyé un e-mail à l'ensemble de ses membres en omettant de cacher l'identité des destinataires. L'al. 2 peut également s'appliquer si le préposé considère que la fourniture de conseils au responsable du traitement concerné peut constituer une mesure suffisante pour remédier à une situation en soi peu problématique.

Al. 3 Devoirs de collaboration

L'al. 3 règle le devoir de collaboration de la personne privée et de l'organe fédéral, en reprenant la réglementation prévue aux art. 27, al. 3, et 29, al. 2, LPD. En vertu de cette disposition, la partie à la procédure d'enquête doit fournir au préposé tous les renseignements et documents qui lui sont nécessaires pour son enquête. La *seconde phrase* de l'al. 3 prescrit que le droit de refuser de fournir des renseignements est régi par les art. 16 et 17 PA. L'art. 16, al. 1, PA renvoie à l'art. 42, al. 1 et 3, de la loi fédérale du 4 décembre 1947 de procédure civile fédérale[177]. Cette disposition prévoit que les personnes interrogées sur des faits dont la révélation les exposerait à des poursuites pénales peuvent refuser de témoigner. Il s'agit des personnes visées aux art. 321, 321bis et 321ter, CP. Ainsi, les médecins peuvent par exemple refuser de fournir au préposé les données personnelles concernant leurs patients sous réserve de leur consentement; il en va de même des avocats par rapport à leurs clients. L'art. 90 du règlement (UE) 2016/679 prévoit également que les Etats membres peuvent adopter des règles spécifiques afin de définir les pouvoirs des autorités de contrôle à l'égard des responsables du traitement et des sous-traitants qui sont soumis en vertu du droit national à une obligation de secret professionnel ou d'autres obligations de secret équivalentes.

Art. 44 Pouvoirs

Cette disposition correspond aux exigences de l'art. 12bis, par. 2, let. a, P-STE 108, qui prescrit que l'autorité de contrôle doit disposer de pouvoirs d'investigation et d'intervention. L'art. 47, par. 1, de la directive (UE) 2016/680 prescrit en outre que les Etats Schengen sont tenus de prévoir que l'autorité de contrôle dispose de pouvoirs d'enquête, notamment celui d'obtenir du responsable du traitement l'accès à toutes les données traitées et à toutes les informations nécessaires pour l'exercice de ses tâches. Quant au règlement (UE) 2016/679, il prévoit une réglementation analogue à son art. 58, par. 1, let. e et f.

Al. 1 Mesures d'investigation

Les mesures énumérées à l'al. 1 ne peuvent être ordonnées que si une procédure d'enquête a été ouverte et pour autant que la personne privée ou l'organe fédéral ne respecte pas son obligation de collaborer. En d'autres termes, ce n'est que si ses tentatives d'obtenir la collaboration du responsable du traitement sont restées vaines que le préposé pourra ordonner les mesures prévues aux let. a à d.

177 RS **273**

Le catalogue des mesures prévues à l'al. 1 est semblable à celui de l'art. 12 PA. Il s'agit d'une liste non exhaustive. Parmi les attributions, le préposé peut ordonner l'accès à tous les renseignements, documents, registres d'activités et données personnelles nécessaires pour l'enquête (*let. a*) ou encore l'accès aux locaux et aux installations (*let. b*). Comme toute autorité fédérale, le préposé doit respecter les dispositions légales applicables, notamment celles de protection des données et celles garantissant la confidentialité des secrets d'affaires et de fabrication. Il est également soumis au secret de fonction au sens de l'art. 22 LPers. La confidentialité des données personnelles auxquelles il a accès dans l'exercice de ses tâches de surveillance est ainsi garantie, notamment lorsqu'il informe l'auteur d'une dénonciation de la suite donnée à celle-ci (art. 43, al. 4) ou lorsqu'il publie son rapport d'activités en vertu de l'art. 51 P-LPD.

Al. 2 Mesures provisionnelles

Cette disposition confère au préposé la compétence d'ordonner des mesures provisionnelles pour la durée de l'enquête et les faire exécuter, le cas échéant, par une autre autorité fédérale ou par des organes de police cantonaux ou communaux. Actuellement, l'art. 33, al. 2, LPD prescrit que si le préposé constate à l'issue de son enquête à l'encontre d'une personne privée ou d'un organe fédéral que la personne concernée risque de subir un préjudice difficilement réparable, il peut requérir des mesures provisionnelles du président de la cour du Tribunal administratif fédéral, qui est compétente en matière de protection des données. Vu que l'art. 45 P-LPD confère des compétences décisionnelles au préposé, l'intervention du Tribunal administratif fédéral pour ordonner des mesures provisoires peut être supprimée. La procédure de recours contre les mesures provisionnelles est régie aux art. 44 ss PA. L'art. 55 PA règle l'effet suspensif du recours.

L'octroi de pouvoirs d'enquête au préposé est un élément déterminant au sens de l'art. 45 du règlement (UE) 2016/679 pour décider du renouvellement ou, le cas échéant, du maintien de la décision d'adéquation de la Commission européenne en faveur de la Suisse.

Art. 45 Mesures administratives

L'art. 45 P-LPD met en œuvre l'art. 47, par. 2, de la directive (UE) 2016/680 et donne suite aux recommandations des évaluateurs Schengen de conférer des compétences décisionnelles au préposé. L'art. 58, par. 2, du règlement (UE) 2016/679 énumère toutes les mesures correctrices que l'autorité de contrôle est habilitée à prendre. En sus de celles prévues à l'art. 47, par. 2, de la directive (UE) 2016/680, l'autorité de contrôle en matière de protection des données dispose notamment du pouvoir de prononcer des amendes administratives (art. 58, par. 2, let. i) et d'ordonner la suspension de flux de données à un destinataire situé dans un Etat tiers ou à un organisme international (art. 58, par. 2, let. j).

L'art. 45 P-LPD est compatible avec l'art. 12bis, par. 2, let. c, et 6, P-STE 108.

Le Conseil fédéral propose néanmoins de ne pas conférer au préposé le pouvoir d'infliger des sanctions administratives, mais de lui conférer la compétence de prononcer un certain nombre de mesures administratives qui, en cas de non-respect, pourront être sanctionnées pénalement (art. 57 P-LPD).

L'art. 45 P-LPD laisse une grande marge de manœuvre au préposé. En effet, cette disposition ne l'oblige pas à prendre des mesures administratives, mais lui donne la faculté de le faire. Cette disposition contient deux catégories de mesures.

La première catégorie prévoit un catalogue de mesures contre des traitements de données contraires à des dispositions de protection des données (al. 1, 2 et 4). Ces mesures vont du simple avertissement (*al. 4*) jusqu'à l'ordre de détruire des données personnelles (*al. 1*) ou à l'interdiction de communiquer des données personnelles à l'étranger (*al. 2*). Le principe de base de cette réglementation est le respect du principe de proportionnalité. Ainsi, au lieu d'ordonner la cessation du traitement, le préposé peut ordonner sa modification et limiter la mesure à la partie du traitement problématique. Il peut également se limiter à prononcer un avertissement si la partie à l'enquête a pris les mesures nécessaires au rétablissement d'une situation conforme aux prescriptions de protection des données (*al. 4*).

La seconde catégorie concerne des cas de non-observation de prescriptions d'ordre ou de devoirs à l'égard de la personne concernée (*al. 3*). Parmi les compétences décisionnelles qui sont attribuées au préposé, celui-ci peut ordonner à l'organe fédéral ou à la personne privée d'établir une analyse d'impact relative à la protection des données personnelles au sens de l'art. 20 (*let. d*) ou de communiquer à la personne concernée les renseignements demandés selon l'art. 23 (*let. g*). La liste de l'al. 3 n'est pas exhaustive.

Le préposé notifie sa décision uniquement aux parties à la procédure d'enquête. Le cas échéant, il informe le public conformément à l'art. 51, al. 2, P-LPD. La mesure prononcée doit être motivée de manière précise. Le responsable du traitement concerné doit en effet être en mesure de déterminer les traitements tombant sous le coup de la décision du préposé. Les parties à la procédure d'enquête ont qualité pour recourir conformément aux dispositions générales sur la procédure fédérale (voir ci-après art. 46). Le cas échéant, le préposé peut assortir la mesure prononcée à l'encontre du responsable du traitement d'une menace pénale (art. 57).

Art. 46 Procédure

Conformément à l'*al. 1*, la procédure d'enquête et celle de décision sur les mesures visées aux art. 44 et 45 sont régies par la PA. La personne privée ou l'organe fédéral partie à l'enquête ont en particulier le droit d'être entendu (art. 29 ss PA).

L'*al. 2* précise que seul l'organe fédéral ou la personne privée contre qui une enquête est ouverte a qualité de partie à la procédure. Par conséquent, seuls ceux-ci peuvent recourir contre les mesures prononcées contre eux par le préposé. La personne concernée n'a pas qualité de partie à la procédure, même si le préposé a ouvert l'enquête sur dénonciation de celle-ci. Dans la mesure où la personne concernée entend faire valoir des prétentions à l'encontre de la personne privée, elle doit agir en justice selon l'art. 28 P-LPD, c'est-à-dire devant le juge civil compétent. Dans le secteur public, la personne concernée doit agir contre l'organe fédéral res-

ponsable (art. 37), en recourant le cas échéant contre la décision de celui-ci auprès de l'autorité de recours compétente. Cette conséquence est inchangée par rapport au droit en vigueur.

Quant à l'*al. 3*, il prescrit que le préposé a qualité pour recourir contre les décisions sur recours du Tribunal administratif fédéral auprès du Tribunal fédéral, comme c'est du reste déjà le cas aujourd'hui en vertu des art. 27, al. 6, et 29, al. 4, LPD.

Art. 47 Coordination

Certaines autorités fédérales exercent des tâches de surveillance sur des privés ou sur des organismes extérieurs à l'administration fédérale. Tel est le cas par exemple de l'Office fédéral de la santé publique par rapport aux assurances maladies, ou de l'Autorité fédérale de surveillance des marchés financiers (FINMA) concernant les banques ou d'autres prestataires financiers. La notion d'«organisation extérieure à l'administration fédérale» correspond à celle prévue à l'art. 1, al. 2, let. e, PA.

Des questions de protection des données personnelles peuvent se poser dans le cadre d'une procédure de surveillance qui peut, le cas échéant, aboutir à une décision de l'autorité compétente. Pour tenir compte de cette problématique, l'*al. 1* prévoit que l'autorité de surveillance est tenue d'inviter le préposé à prendre position. Dans l'hypothèse où ce dernier a également ouvert une enquête au sens de l'art. 43 P-LPD contre la même partie, l'*al. 2* prescrit que l'autorité de surveillance et le préposé doivent se coordonner sur deux plans: d'une part pour déterminer si les deux procédures peuvent être menées parallèlement, ou si une des deux doit être suspendue ou encore abandonnée, et d'autre part sur le contenu de leur décision respective dans l'hypothèse où les procédures sont menées parallèlement. En cas de conflit de compétences, le Conseil fédéral tranchera (art. 9, al. 3, PA). La coordination doit être assurée de manière simple et rapide. Les entités concernées doivent être informées de l'issue de cette coordination et de la législation applicable, afin qu'elles soient fixées sur leurs droits et obligations dans les meilleurs délais.

9.1.8.3 Assistance administrative

Art. 48 Assistance administrative en Suisse

Cette disposition règle l'assistance administrative entre le préposé et les autorités fédérales et cantonales. Il s'agit d'une nouvelle disposition. L'art. 31, al. 1, let. c, LPD se limite en effet à attribuer au préposé la tâche de collaborer avec les autorités chargées de la protection des données en Suisse.

L'*al. 1* pose le principe selon lequel les autorités fédérales et cantonales sont tenues de communiquer au préposé les informations et les données personnelles nécessaires à l'accomplissement de ses tâches légales. Il s'agit d'une norme standard d'assistance administrative que l'on retrouve dans d'autres lois fédérales.

L'*al. 2* prescrit que le préposé est habilité à communiquer des informations et des données aux autorités cantonales compétentes en matière de protection des données (*let. a*), aux autorités pénales compétentes lorsqu'il s'agit de dénoncer une infraction

conformément à l'art. 59, al. 2, P-LPD (*let. b*), ainsi qu'aux autorités fédérales et aux organes de police cantonaux et communaux pour l'exécution des mesures prévues aux art. 44, al. 2, et 45 P-LPD (*let. c*).

Les communications visées aux al. 1 et 2 peuvent être effectuées spontanément ou sur demande.

Art. 49 Assistance administrative avec des autorités étrangères

Cette disposition règle l'assistance administrative entre le préposé et les autorités étrangères chargées de la protection des données. Il s'agit d'une nouvelle disposition. L'art. 31, al. 1, let. c, LPD se limite en effet à attribuer au préposé la tâche de collaborer avec les autorités étrangères chargées de la protection des données.

Cette disposition transpose l'art. 50 de la directive (UE) 2016/680. Elle correspond également aux exigences des art. 15 et 16 P-STE 108. Le règlement (UE) 2016/679, à l'art. 61, prévoit une réglementation analogue.

Le préposé aurait souhaité que la disposition soit complétée de telle manière qu'il soit habilité à régler les modalités de la collaboration avec les autorités étrangères chargées de la protection des données par le biais de conventions de collaboration. Le Conseil fédéral a estimé qu'il était préférable de s'en tenir à la délégation prévue à l'art. 61 P-LPD.

Al. 1 Conditions

Cette disposition pose le principe selon lequel le préposé peut échanger des données personnelles avec une autorité étrangère chargée de la protection des données pour l'accomplissement de leurs tâches légales respectives, pour autant que certaines conditions, énumérées aux let. a à e, soient remplies.

Selon la première condition (*let. a*), le principe de réciprocité en matière d'assistance administrative dans le domaine de la protection des données doit être garanti entre la Suisse et l'Etat étranger. Deuxièmement, conformément au principe de spécialité, les informations et les données personnelles échangées ne doivent être utilisées que dans le cadre de la procédure liée à la protection des données à la base de la demande d'assistance (*let. b*). Si les données transmises doivent être utilisées ultérieurement dans le cadre d'une procédure pénale, les dispositions sur l'entraide judiciaire internationale en matière pénale s'appliquent. Les troisième et quatrième conditions garantissent le respect des secrets professionnels, d'affaires et de fabrication (*let. c*) et interdisent que les informations et les données échangées soient communiquées à des tiers sans l'accord préalable de l'autorité qui les a transmises (*let. d*). Enfin, l'autorité destinataire doit respecter les restrictions d'utilisation exigées par l'autorité qui lui a transmis les informations (*let. e*).

Le préposé peut refuser la demande d'assistance administrative d'une autorité étrangère par exemple si les conditions de l'art. 13 P-LPD ne sont pas respectées ou si un des motifs prévus à l'art. 32, al. 6, P-LPD s'oppose à la communication des données personnelles.

Al. 2 Communication de données personnelles

L'al. 2 définit aux let. a à g les informations que le préposé peut communiquer à l'autorité étrangère pour motiver sa demande d'assistance administrative ou pour donner suite à une demande étrangère. Pour communiquer l'identité des personnes concernées (*let. c*), le préposé doit obtenir le consentement de chacune d'elles conformément aux exigences de l'art. 5, al. 6, P-LPD (let. c, *ch. 1*). A défaut, ces données peuvent également être communiquées si cela est indispensable à l'accomplissement des tâches légales du préposé ou de l'autorité étrangère (let. c, *ch. 2*). Ces conditions correspondent à celles prévues à l'art. 32, al. 2, let. a et b, P-LPD.

Al. 3 Consultation

Lorsque, dans le cadre d'une procédure d'assistance administrative, le préposé envisage de transmettre à une autorité étrangère chargée de la protection des données des informations susceptibles de contenir des secrets professionnels ou des secrets d'affaires ou de fabrication, il est tenu d'informer les personnes concernées en les invitant à prendre position. Le préposé est néanmoins délié de son obligation si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés.

9.1.8.4 Autres tâches du préposé

Art. 50 Registre

Cette disposition prévoit que le préposé tient un registre des activités de traitements que les organes fédéraux lui ont préalablement annoncées (art. 11, al. 4). Ce registre est publié, comme c'est le cas aujourd'hui.

Art. 51 Information

L'*al. 1* correspond à l'art. 30, al. 1, LPD, sous réserve que le préposé doit dorénavant présenter un rapport annuel à l'Assemblée fédérale et au Conseil fédéral.

L'*al. 2* renforce l'information active du préposé. Celui-ci informe le public de ses constatations et de ses décisions, pour autant toutefois que l'information présente un intérêt général pour le public. La seconde phrase de l'art. 30, al. 2, LPD est supprimée. En tant qu'autorité indépendante, le préposé doit pouvoir déterminer seul le contenu de l'information à fournir au public. Les données doivent être rendues anonymes, à moins qu'il n'existe un intérêt public prépondérant à leur publication (art. 32, al. 3 et 5, P-LPD). Les conditions de l'art. 32, al. 6, P-LPD s'appliquent pour le surplus.

L'obligation pour l'autorité de contrôle d'établir un rapport d'activité est prévue à l'art. 49 de la directive (UE) 2016/680 et à l'art. 12bis, par. 5bis, P-STE 108. Le règlement (UE) 2016/679, à l'art. 59, prévoit une réglementation analogue.

Art. 52 Autres attributions

Par rapport au droit en vigueur (art. 31 LPD), la liste des compétences attribuées au préposé est complétée afin de mettre en œuvre l'art. 46, par. 1, let. d. et e, de la directive (UE) 2016/680. Ces nouvelles attributions correspondent également aux exigences de l'art. 12bis, ch. 2, let. e, P-STE 108.

En vertu de l'*al. 1*, le préposé a en particulier pour tâche d'informer, de former et de conseiller les organes fédéraux et les personnes privées dans le domaine de la protection des données. Cela englobe l'organisation de manifestations à but informatif ainsi que celle de formations continues, notamment pour les responsables du traitement dans le secteur public (*let. a*). Le préposé doit par ailleurs aussi sensibiliser le public, et en particulier les personnes vulnérables telles que les personnes mineures ou les personnes âgées, à la protection des données (*let. c*). Il doit également fournir aux personnes concernées, sur demande, des informations sur l'exercice de leurs droits (*let. d*).

En vertu de la *let. e*, le préposé doit être consulté sur tous les projets d'actes législatifs et de mesures fédérales qui impliquent des traitements de données personnelles, et non plus seulement sur les projets touchant de manière importante à la protection des données. Cette modification correspond à la pratique actuelle.

La *let. g* prévoit que le préposé a aussi comme attribution d'élaborer des guides et des outils à l'attention des responsables du traitement, des sous-traitants et des personnes concernées. C'est une tâche qu'il exécute déjà aujourd'hui dans le cadre de son activité de conseil (art. 28, 30 et 31 LPD)[178]. La *let. g* précise qu'il doit tenir compte des particularités des différents secteurs concernés, ainsi que du besoin de protection accru des personnes particulièrement vulnérables, telles que les mineurs, les personnes en situation de handicap ou les personnes âgées.

L'*al. 2* correspond à l'art. 31, al. 2, LPD.

Abrogation de l'art. 33 LPD

Cette disposition peut être supprimée. L'al. 1, qui prescrit que les voies de droit sont régies par les dispositions générales de la procédure fédérale, n'a en effet qu'une portée déclaratoire. Quant à l'al. 2, il est superflu vu l'art. 44, al. 2, P-LPD.

9.1.8.5 Emoluments

Art. 53

Actuellement, l'art. 33, al. 1, OLPD dispose que les avis fournis aux personnes privées par le préposé sont soumis à émolument et que l'ordonnance générale du 8 septembre 2004 sur les émoluments (OGEmol)[179] s'applique pour le surplus.

178 Par exemple: guide pour le traitement des données dans le domaine médical, guide pour le traitement des données dans l'administration fédérale, guide pour le traitement dans le secteur du travail.

179 RS **172.041.1**

L'*al. 1* prévoit de fixer au niveau de la loi le principe selon lequel le préposé est tenu de percevoir un émolument pour certaines prestations fournies aux personnes privées, à savoir la prise de position sur les codes de conduite (*let. a*), l'approbation des clauses type de protection des données et des règles d'entreprise contraignantes (*let. b*), l'examen de l'analyse d'impact relative à la protection des données (*let. c*), les mesures prononcées en vertu des art. 44, al. 2, et 45 P-LPD (*let. d*), ainsi que la fourniture de conseils en matière de protection des données (*let. e*). Il résulte a contrario de l'al. 1 qu'une enquête clôturée sans que des mesures provisionnelles ou administratives n'aient dû être prises, n'est soumise à aucun émolument.

L'*al. 2* charge le Conseil fédéral de fixer le montant des émoluments. Conformément aux exigences de l'art. 46*a*, al. 1, LOGA, celui-ci doit d'une part prévoir des émoluments uniquement pour les actes déterminés à l'art. 53, al. 1 P-LPD; il doit d'autre part fixer le montant des émoluments de telle manière qu'ils couvrent les coûts découlant de ces actes (principe de la couverture des coûts). Il n'est donc pas prévu de financer l'ensemble de l'activité du préposé par la perception d'émoluments, mais uniquement de couvrir l'ensemble des frais engendrés par les actes mentionnés à l'al. 1. Dans le cadre de sa réglementation, il est envisageable que le Conseil fédéral prévoie un tarif horaire ou forfaitaire en fonction de la prestation fournie.

L'*al. 3* permet au surplus au Conseil fédéral de déterminer les cas dans lesquels le préposé peut renoncer à percevoir des émoluments ou les réduire. Par exemple, il est possible d'envisager une exception lorsque la prestation sert un intérêt public prépondérant, contribuant au respect des prescriptions de protection des données. L'art. 3, al. 2, let. a, OGEmol prévoit une solution analogue. En outre, une autre solution envisageable est de conférer au préposé la faculté d'accorder un sursis de paiement, de réduire les émoluments ou de procéder à une remise si le responsable du traitement ou le sous-traitant est une personne physique ou une petite ou moyenne entreprise.

La perception des émoluments ne vaut qu'à l'égard des personnes privées. En ce qui concerne les conseils fournis aux autorités cantonales, l'art. 3, al. 1, OGEmol s'applique: l'administration fédérale ne perçoit pas d'émoluments des organes intercantonaux, des cantons et des communes, pour autant qu'ils accordent la réciprocité à la Confédération. Les prestations fournies aux organes fédéraux sont gratuites.

9.1.9 Dispositions pénales

Compte tenu des nombreuses prises de position critiques envers l'avant-projet, le Conseil fédéral a fondamentalement remanié les dispositions pénales.

Lors de la consultation externe, l'introduction de sanctions administratives pécuniaires a été réclamée (en référence au règlement UE 2016/679). En Suisse, les sanctions administratives pécuniaires à caractère punitif ont un caractère exceptionnel. Elles appartiennent typiquement aux domaines dans lesquels des entreprises exercent une activité économique nécessitant une concession ou une autorisation, ou bénéficiant de subventions étatiques, et sont soumises à une surveillance administrative (poste, jeux d'argent et agriculture notamment). Elles ont de surcroît été intro-

duites en droit des cartels à une époque où le code pénal ne connaissait pas encore de responsabilité pénale de l'entreprise. De telles sanctions administratives pécuniaires revêtent un caractère pénal qui implique le respect de certaines garanties de procédure pénale. La procédure administrative applicable ne règle cependant pas ces questions. A cela s'ajoute que ces sanctions consistent à imputer directement à une entreprise la faute commise par un tiers. Or, le législateur a précisément rejeté cette solution en réglant la punissabilité de l'entreprise à l'art. 102 CP: la responsabilité de l'art. 102 CP n'est ni une responsabilité causale, ni une responsabilité à raison du risque[180], mais repose sur l'exigence d'un manque spécifique d'organisation. L'introduction de sanctions administratives à caractère pénal dans la LPD réduirait fortement la portée de cette décision de principe du droit pénal par la voie détournée du droit administratif.

De telles sanctions administratives s'avéreraient en outre particulièrement délicates dans le domaine de la protection des données. Le champ d'application de la LPD est beaucoup plus étendu que celui des lois régissant les domaines dans lesquels on trouve traditionnellement des sanctions administratives pécuniaires et où l'activité économique est exercée par des entreprises. La LPD s'adresse certes aussi aux grandes entreprises, mais elle touche également les petites et moyennes entreprises, ainsi que les personnes physiques. Le fait qu'il n'existe aucun droit de procédure codifié pour les sanctions administratives à caractère pénal implique entre autres le risque de saper les droits procéduraux des personnes physiques. C'est d'autant plus vrai que le droit pénal accessoire connaît des différences entre les droits procéduraux des personnes physiques et ceux des personnes morales[181]. En résumé, l'introduction de sanctions administratives pécuniaires dans la LPD s'accompagnerait d'une grande insécurité juridique, ce qui n'est guère défendable, et pas uniquement dans le domaine de la protection des données.

C'est pourquoi le Conseil fédéral veut recourir à des structures bien établies et riches d'une solide pratique. En Suisse, le respect des obligations fondamentales du droit administratif est assuré par le droit pénal administratif ou le droit pénal accessoire. Les destinataires des normes sont les personnes physiques. Lorsque l'obligation administrative incombe à l'entreprise, sa violation est imputée aux personnes occupant une fonction dirigeante (cf. art. 29 CP et 6 DPA[182]). La crainte exprimée lors de la consultation de voir condamné n'importe quel employé d'une entreprise s'avère ainsi infondée. Le recours à des sanctions de droit pénal implique aussi que les gains résultant d'infractions pénales à la LPD ainsi que les instruments du délit peuvent être confisqués en application des dispositions du CP (art. 69 ss CP). Enfin, il n'est pas souhaitable que le préposé prononce des sanctions pénales, car cela nécessiterait de modifier fondamentalement son organisation et de la développer de manière importante. Le Conseil fédéral donne dès lors la préférence au système de poursuite pénale existant.

Le dispositif pénal de la LPD doit être renforcé par rapport au droit en vigueur. Les sanctions doivent être dissuasives, comme l'exigent le P-STE 108 (art. 10) et la

180 Message PG-CP, FF **1999** II 1787 ss, ch. 217.421, et ATF **142** IV 333.
181 Sur l'application du principe *nemo tenetur* aux personnes morales en droit pénal accessoire, cf. ATF **142** IV 207, 215 s. et 222 s., et ATF **140** II 384, 393.
182 Voir à ce sujet ATF **142** IV 315.

Directive (UE) 2016/680 (art. 57). Un système pénal trop clément peut avoir pour conséquence que la réglementation suisse ne soit plus jugée suffisante par l'UE. Le système de sanctions proposé présente les caractéristiques principales suivantes:

- Il renonce à pénaliser la violation des obligations administratives commises par négligence, suivant ainsi les dernières décisions du Parlement (concernant par ex. le projet de loi fédérale sur les jeux d'argent[183]). Le préposé aurait quant à lui souhaité que la négligence soit punie.
- Les obligations du droit administratif sont précisées et leur pénalisation est limitée aux devoirs essentiels.
- A titre de compensation, le préposé se voit attribuer la compétence de prononcer des décisions ordonnant le respect des obligations de la LPD sous menace de sanctions pénales en cas d'insoumission. Ce modèle est largement répandu en droit pénal accessoire (par ex. dans la loi fédérale du 22 juin 2007 sur l'Autorité fédérale de surveillance des marchés financiers [LFINMA][184]) et correspond au mécanisme de l'art. 292 CP. Au besoin, le préposé peut participer à la procédure pénale cantonale en tant que partie plaignante.
- Le Conseil fédéral fixe le montant maximal de l'amende à 250 000 francs. Cette augmentation intervient en particulier pour se rapprocher du règlement (UE) 2016/679. Il serait en revanche discutable de fixer un montant maximal plus important pour les personnes physiques au motif que des amendes peu élevées ne seraient pas dissuasives pour les entreprises. Les dispositions pénales de la LPD s'adressent avant tout aux personnes physiques, plus particulièrement à celles qui occupent des fonctions dirigeantes (cf. art. 29 CP et 6 DPA). Il faut relever que, dans la LFINMA par exemple, la violation par négligence des obligations administratives est punie d'une amende de 250 000 francs au plus (art. 44 ss LFINMA), tandis que le non-respect d'une décision est sanctionné d'une amende de 100 000 francs au plus (art. 48 LFINMA). Le préposé estime pour sa part que les amendes ne sont pas suffisamment dissuasives eu égard notamment à leur montant.
- La violation du devoir de discrétion demeure, comme jusqu'à présent, une contravention.
- Lorsque les données sont traitées par une entreprise, les obligations de la LPD incombent, en règle générale, aux dirigeants de cette dernière, qui sont alors légalement tenus d'en assurer le respect[185]. La violation de ces obligations ou l'insoumission à une décision du préposé adressée à l'entreprise sont dès lors imputées aux dirigeants de l'entreprise et non aux simples exécutants, en application des art. 29 CP et 6 DPA.
- Lorsque l'amende n'excède pas 50 000 francs, les entreprises peuvent être directement sanctionnées en application de l'art. 7 DPA. Cela permet de tenir compte des critiques formulées lors de la consultation.

183 FF **2015** 7769
184 RS **956.1**
185 Cf. ATF **142** IV 315.

Art. 54 Violation des obligations d'informer, de renseigner et de collaborer

L'art. 54 P-LPD reprend l'art. 34 LPD, à l'exception de l'art. 34, al. 2, let. a, LPD, car les obligations correspondantes n'existent plus dans le P-LPD. Il inclut en revanche le nouveau devoir d'informer en cas de décision individuelle automatisée (art. 19 P-LPD).

Tombe sous le coup de l'*al. 1*, *let. a*, le fait de fournir intentionnellement un renseignement inexact, mais aussi le fait de donner des informations incomplètes tout en laissant croire que celles-ci sont complètes. Le fait de ne fournir aucune information n'est pas punissable en application de la let. a, mais de la let. b le cas échéant. Toutefois, la personne privée qui, contre la vérité, prétend ne détenir aucune information sur la personne concernée, est punissable selon l'al. 1, let. a.

L'al. 1, *let. b*, vise les cas dans lesquels la personne privée omet complètement d'informer la personne concernée conformément à l'art. 17, al. 1, et 19, al. 1, ou de lui donner les informations prévues à l'art. 17, al. 2. N'est pas punissable la personne privée qui, invoquant l'art. 18 ou 25, prétend qu'elle n'est pas tenue de fournir de renseignements. Dans ce cas, en effet, la personne concernée sait qu'un traitement a lieu. Elle est donc en mesure de faire valoir ses droits et d'intenter une action de droit civil qui déterminera si le refus ou la restriction du droit d'accès et du devoir d'information est justifiée ou non[186].

L'*al. 2* reprend l'art. 34, al. 2, let. b, LPD qui punit le fait de donner des renseignements faux ou de refuser de collaborer dans le cadre d'une enquête.

La violation de ces obligations doit continuer à constituer une contravention, mais il convient d'élever significativement le montant maximal de l'amende en le fixant à 250 000 francs. La peine effective sera déterminée en tenant compte de la situation économique de l'auteur (art. 106, al. 3, CP, en relation avec l'art. 47 CP). Dans les cas de peu de gravité, l'entreprise peut être condamnée au paiement de l'amende en lieu et place de la personne physique responsable. Il est de plus possible, dans ces cas, de renoncer à la poursuite ou à la condamnation aux conditions de l'art. 52 CP.

Art. 55 Violation des devoirs de diligence

Cette disposition est nouvelle. Elle est nécessaire, parce que le P-LPD prévoit de nouvelles obligations élémentaires qui ne sont pas couvertes par les dispositions pénales du droit en vigueur. Une protection efficace de la personnalité des personnes concernées est uniquement possible si le responsable du traitement et le sous-traitant satisfont à leurs devoirs. Afin que ceux-ci y soient tenus, le Conseil fédéral propose cette extension des dispositions pénales.

De par sa nature, cet article devrait avant tout s'adresser aux personnes disposant d'un pouvoir de direction, car la compétence de décider du respect des devoirs de diligence est une tâche de direction (cf. également l'art. 29 CP).

186 Voir aussi FF **1988** 421, 490.

Art. 56 Violation du devoir de discrétion

Depuis l'entrée en vigueur de la LPD, les technologies de l'information et de la communication ont énormément évolué et pris une importance considérable. De plus en plus de données sont enregistrées et traitées par un nombre toujours croissant de personnes sur toujours davantage d'appareils, notamment en raison de la propagation massive des téléphones intelligents. Dans ce contexte, il est indiqué d'étendre le devoir de discrétion à toutes les données personnelles. Ce qui est décisif, c'est qu'il s'agisse de données secrètes. Cela correspond aux art. 320 et 321 CP, pour lesquels le fait de savoir si l'information en question est secrète ou non constitue le critère déterminant. C'est ainsi la notion matérielle de secret du droit pénal qui est pertinente[187]. Constitue un secret protégé par le droit pénal tout fait qui n'est pas largement connu ni accessible à tout un chacun, dont la publicité limitée est voulue par le maître du secret et à la confidentialité duquel ce dernier a un intérêt digne de protection. C'est dire que n'importe quelle divulgation de données personnelles ne réalise pas l'infraction. La notion de «révélation» correspond à celle des art. 320 et 321 CP, ce qui assure la cohérence du point de vue du comportement punissable[188].

L'art. 56 permet de combler les lacunes qui résultent du cercle restreint des auteurs touchés par les art. 320 et 321 CP (délits propres). C'est pourquoi il impose un devoir de discrétion également aux personnes qui ne tombent pas sous le coup des art. 320 ou 321 CP. La violation du devoir de discrétion est une contravention (poursuivie sur plainte) punie d'une amende de 250 000 francs au plus (*al. 1*).

L'*al. 2* étend la punissabilité aux auxiliaires (les sous-traitants de données) et aux personnes en formation. Cette extension correspond au droit en vigueur ainsi qu'à la réglementation de l'art. 321 CP («auxiliaires»). Le Conseil fédéral a proposé au Parlement de modifier l'art. 320 CP dans le même sens avec le message concernant la loi sur la sécurité de l'information[189].

La révélation des données peut être justifiée par l'autorisation de la personne concernée. Les règles générales, ainsi que les principes développés par la jurisprudence et la doctrine dans le cadre de l'art. 321, ch. 2, CP, s'appliquent par analogie[190].

Dans la pratique, il est possible que des questions de concours se posent, en particulier avec l'art. 320 CP (fonctionnaires fédéraux) et l'art. 321 CP (avocats, médecins, etc.). Cependant, tel est déjà le cas du droit en vigueur, de sorte que cela ne devrait pas poser de problèmes particuliers.

Art. 57 Insoumission à une décision

Le Conseil fédéral a introduit l'art. 57 après la consultation. Le droit pénal accessoire contient beaucoup de dispositions analogues. Cet article sert, d'une part, à compenser l'abandon de nombreuses dispositions pénales par rapport à l'AP-LPD.

187 Stefan/Jean-Richard-dit-Bressel Marc, in: Trechsel/Pieth (éd.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurich/St-Gall 2013, n. 2 ad art. 162 CP.
188 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (éd.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurich/St-Gall 2013, n. 8 ad art. 320 CP et n. 23 s. ad art. 321 CP.
189 FF **2017** 2765, 2812 s. et 2886 ss
190 Trechsel Stefan/Vest Hans, in: Trechsel/Pieth (éd.), Schweizerisches Strafgesetzbuch Praxiskommentar, Zurich/St-Gall 2013, n. 28 ad art. 321 CP.

D'autre part, il permet de résoudre les questions liées au principe *nulla poena sine lege* qui ont souvent été mises en avant lors de la consultation. Les mêmes questions se seraient posées avec des sanctions administratives, dans la mesure où celles-ci revêtent un aspect pénal. La présente solution permet de continuer à formuler les obligations du P-LPD de manière suffisamment générale et abstraite, tout en évitant de heurter les exigences du droit pénal relatives à la précision de la base légale. Ce modèle simplifie de surcroît le travail des autorités de poursuite pénale et tient ainsi compte des préoccupations émises par une partie des participants à la consultation.

Avec l'art. 57, le préposé peut prononcer une décision ordonnant le respect des obligations inscrites dans le P-LPD (cf. art. 45, al. 3), sous la menace d'une peine en cas d'insoumission. Ce modèle présente l'avantage de permettre de décrire de la manière la plus concrète possible, dans la décision, l'obligation que le destinataire doit respecter, de sorte qu'il ne subsiste pour ce dernier aucun doute quant à ce qu'il doit faire ou ne pas faire. Cela facilite en outre le travail des autorités de poursuite pénale cantonales chargées, sur dénonciation du préposé en cas d'insoumission, d'établir l'état de fait et de prononcer un jugement ou une ordonnance pénale.

Lorsque la décision du préposé s'adresse à une entreprise, c'est une personne occupant une fonction dirigeante qui est punissable selon l'art. 29 CP: le devoir qui fonde la punissabilité et qui incombe à l'entreprise est imputé à la personne physique. Cela permet également de tenir compte de certaines critiques émises lors de la consultation.

Art. 58 Infractions commises dans une entreprise

L'art. 58 rend les art. 6 et 7 DPA applicables. Un renvoi exprès est nécessaire, car la DPA est en principe inapplicable en l'espèce.

L'art. 6, al. 2, DPA, permet de rendre le chef d'entreprise responsable également dans le domaine de la LPD. Les obligations de la LPD devraient en effet, en règle générale, s'adresser au chef d'entreprise[191]. L'art. 6, al. 2, DPA, remplit ainsi une fonction analogue à celle de l'art. 29 CP et attribue la responsabilité pénale à la direction de l'entreprise, c'est-à-dire aux personnes occupant une fonction dirigeante et disposant de pouvoirs de décision et de direction. Cela permet d'imputer de manière appropriée la responsabilité pénale au sein des entreprises.

Le montant maximal de l'amende au paiement duquel il est possible de condamner une entreprise à la place de la personne physique responsable selon l'art. 7 DPA est relevé à 50 000 francs. Cette adaptation est nécessaire, car le montant maximal des amendes de la LPD n'est pas 10 000 francs (art. 106, al. 1, CP) mais 250 000 francs.

Art. 59 Compétence

Comme actuellement, la poursuite et le jugement des infractions incombent en principe aux cantons. Le préposé peut dénoncer les infractions et faire valoir les droits de la partie plaignante dans la procédure pénale (art. 118 ss CPP). Il peut ainsi s'opposer aux décisions de classement et interjeter appel des jugements lorsque cela

191 Cf. ATF **142** IV 315.

semble nécessaire pour assurer une application uniforme de la LPD. Il ne peut en revanche faire valoir aucune voie de droit à l'encontre des ordonnances pénales ni de la mesure de la peine, ce qui ne paraît pas nécessaire à l'accomplissement de ses tâches.

Art. 60 Prescription de l'action pénale

Selon l'art. 109 CP, l'action pénale se prescrit par trois ans en cas de contravention. Les instructions en matière de protection des données requièrent des connaissances technologiques et peuvent nécessiter beaucoup de temps. Afin d'éviter que les procédures pénales en matière de protection des données ne soient vouées à l'échec en raison d'un délai de prescription trop court, le Conseil fédéral prévoit de porter ce délai à cinq ans.

9.1.10 Conclusion de traités internationaux

Art. 61

Cette disposition remplace l'art. 36, al. 5, de la loi actuelle, qui est trop vague eu égard aux principes en vigueur en matière de délégation de compétences. Cette disposition précise que le Conseil fédéral peut conclure des traités internationaux avec un ou plusieurs autres sujets de droit international (pays, organisation internationale) dans deux cas. En vertu de la *let. a*, le Conseil fédéral peut conclure des traités concernant la coopération entre autorités de protection des données. On vise par là des accords de coopération sur le modèle de l'accord du 17 mai 2013 entre la Confédération suisse et l'Union européenne concernant la coopération en matière d'application de leurs droits de la concurrence[192]. En vertu de la *let. b*, le Conseil fédéral peut également conclure des traités concernant la reconnaissance réciproque du niveau de protection adéquat en cas de communication transfrontière de données.

Les autres alinéas de l'art. 36 LPD sont abrogés: les al. 1 et 4 sont superflus, dans la mesure où la pratique de prévoir expressément que le Conseil fédéral doit édicter des dispositions d'exécution a été abandonnée. L'al. 3, qui prescrit que le Conseil fédéral peut prévoir des dérogations aux art. 8 et 9 LPD en ce qui concerne l'octroi de renseignements par les représentations diplomatiques et consulaires suisses à l'étranger, peut aussi être supprimé. Enfin, l'al. 6 est inutile, dans la mesure où le Conseil fédéral n'a jamais fait usage de sa compétence de régler la manière de mettre en sûreté les fichiers dont les données, en cas de guerre ou de crise, sont de nature à mettre en danger la vie ou l'intégrité corporelle des personnes concernées.

192 RS **0.251.268.1**. Notons que dans ce cas, le Conseil fédéral n'avait pas de délégation de compétence.

9.1.11 Dispositions finales

Abrogation de l'art. 37 LPD

Il ressort de la consultation externe que l'art. 37 LPD est superflu et doit donc être supprimé. Aujourd'hui, tous les cantons disposent d'une législation assurant un niveau de protection des données adéquat au regard des exigences de la convention STE 108 et de son protocole additionnel.

Art. 62 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont commentées sous ch. 9.2.

Art. 63 Dispositions transitoires concernant les obligations du responsable du traitement

Selon l'*al. 1*, le devoir d'information lors de collectes de données personnelles dépend de l'ancien droit pendant deux ans suivant l'entrée en vigueur de la présente loi. Les responsables privés doivent pendant deux ans informer la personne concernée seulement en cas de collecte de données sensibles (art. 14 LPD). Le devoir d'information sur la collecte de profils de la personnalité, qui existe selon l'ancien droit, tombe, car il n'y a plus de profils de la personnalité selon le nouveau droit. Les organes fédéraux doivent informer les personnes concernées de la collecte de données personnelles selon l'ancien droit (art. 18 LPD), sauf si l'art. 63, al. 2, P-LPD est applicable.

Selon l'*al. 2*, les art. 6 et 17 à 21 ne sont valables pendant les deux ans qui suivent l'entrée en vigueur de la loi que pour les traitements selon les art. 1 et 2 de la directive (UE) 2016/680. Pour les responsables du traitement privés et les organes fédéraux qui traitent de données hors du champ d'application de la directive (UE) 2016/680, ces articles s'appliqueront seulement deux ans après l'entrée en vigueur de la loi. Cette règle veut laisser aux responsables du traitement suffisamment de temps pour se préparer à ces nouveaux devoirs. Dans le champ d'application de la directive (UE) 2016/680, ces articles s'appliquent dès l'entrée en vigueur de la loi.

Art. 64 Dispositions transitoires concernant les traitements

L'art. 64 contient plusieurs règles de droit transitoire sur la question du traitement.

Al. 1

L'al. 1 concerne les traitements de données qui seront terminés au moment de l'entrée en vigueur de la présente loi. Il s'agit des traitements de données effectués sous l'ancien droit et qui ne se poursuivent pas après l'entrée en vigueur du nouveau droit. De tels traitements dépendent entièrement de l'ancien droit. Ainsi, des traitements de données terminés qui étaient licites selon l'ancien droit ne peuvent pas devenir illicites selon le nouveau droit. Il faut encore différencier ici le droit d'accès (art. 23 à 25): après l'entrée en vigueur du nouveau droit, il dépendra exclusivement du nouveau droit et ce, même en ce qui concerne les données et les traitements qui auront été entièrement effectués sous l'ancien droit.

Al. 2

L'al. 2 concerne les traitements de données commencés sous l'ancien droit et qui perdurent après l'entrée en vigueur du nouveau droit, dont le nouveau droit a cependant durci les conditions. On peut penser par exemple à une atteinte à la personnalité selon le nouveau droit, parce que les exigences sur les motifs justificatifs ont changé. Un tel traitement peut continuer en principe pendant deux ans sans autres adaptations. Pendant ce temps, le responsable doit s'assurer que le traitement deviendra conforme au nouveau droit. L'al. 2 ne s'applique cependant pas aux devoirs fixés art. 6, 20 et 21, qui sont réglés par l'al. 3.

Al. 3

L'al. 3 concerne les traitements de données qui ont débuté sous l'ancien droit et qui perdurent après l'entrée en vigueur du nouveau droit. Pour de tels traitements, les art. 6, 20 et 21 ne s'appliquent pas lorsque la finalité du traitement reste inchangée et qu'aucune nouvelle donnée n'est collectée. Dans ce cas, le traitement peut être continué, sans qu'il faille satisfaire aux exigences de l'art. 6. Une évaluation ultérieure sous l'angle de la protection des données n'est pas nécessaire. Cette règle est cohérente dans la mesure où les devoirs des art. 6 et 20 s. s'appliquent surtout dans la phase préliminaire du traitement. Les responsables du traitement ne doivent pas être obligés de les remplir rétroactivement.

Si les conditions d'application de l'al. 3 ne sont pas remplies, les devoirs fixés aux art. 6, 20 et 21 s'appliquent également aux traitements qui auraient commencé sous l'ancien droit et continueraient sous le nouveau. A l'exception du domaine d'application de la directive (UE) 2016/680, les dispositions en question prendraient alors effet deux ans après l'entrée en vigueur de la présente loi, ce qui laisse au responsable du traitement un délai transitoire de deux ans pour se conformer à ces devoirs.

Al. 4

L'al. 4 concerne tous les traitements de données qui ne tombent pas sous le coup des al. 1 à 3. Il s'agit en particulier des traitements qui ont commencé après l'entrée en vigueur de la présente loi, mais aussi ceux qui sont conformes tant à l'ancienne qu'à la nouvelle loi. Pour ces traitements, le nouveau droit s'applique dès l'entrée en vigueur de ses dispositions.

Art. 65 Disposition transitoire concernant les procédures en cours

Pour garantir la sécurité juridique et le respect du principe de la bonne foi, cette disposition prescrit que les enquêtes du préposé pendantes au moment de l'entrée en vigueur de la future LPD, ainsi que les recours contre les décisions de première instance, restent régis par l'ancien droit. Cette notion vise aussi bien les règles matérielles de protection des données que les compétences du préposé, ainsi que les autres normes de procédure applicables.

Art. 66 Disposition transitoire concernant les données des personnes morales

La suppression, dans le P-LPD, de la protection des données concernant des personnes morales et la limitation, à l'art. 4, let. a, P-LPD, de la définition des données

personnelles aux informations concernant une *personne physique* identifiée ou identifiable ont plusieurs conséquences pour les traitements de données effectués par des organes fédéraux. Du fait de ces changements, les dispositions du droit fédéral qui donnent aux organes fédéraux le pouvoir de traiter et de communiquer des données personnelles ne seront plus applicables au traitement et à la communication de données de *personnes morales*. Cependant, en vertu du principe de légalité inscrit à l'art. 5, al. 1, Cst., toute action de l'Etat (y compris le traitement ou la communication de données) nécessite une base légale (voir aussi les art. 13, al. 2, 27 et 36, Cst.). C'est la raison pour laquelle le projet introduit dans la LOGA un ensemble de dispositions régissant le traitement de données de personnes morales par les organes fédéraux (cf. ch. 9.2.8). Citons en particulier l'art. 57*r* P-LOGA, qui crée une base légale générale pour le traitement par des organes fédéraux de données concernant des personnes morales, et l'art. 57*s* P-LOGA, qui, à l'instar de l'art. 32 P-LPD concernant la communication de données personnelles, précise les exigences auxquelles doivent satisfaire les bases légales s'agissant de la communication de données de personnes morales. Contrairement à l'art. 57*r* P-LOGA, l'art. 57*s* P-LOGA ne constitue pas une base légale pour la communication spécifique de données par des organes fédéraux. C'est pourquoi la communication de données concernant des personnes morales devra toujours s'appuyer sur une base légale prévue dans une loi spéciale. Il n'est pas utile d'adapter toutes les bases légales existantes (qui, compte tenu des modifications du P-LPD, ne seront plus applicables qu'aux personnes physiques), car cela allongerait considérablement le projet et le message. Le Conseil fédéral estime qu'il est plus judicieux d'attendre la fin des débats parlementaires sur le présent projet pour réviser à fond les dispositions sur la protection des données instituées par des lois spéciales et voir lesquelles des prescriptions en vigueur relatives au traitement de données de personnes morales par des organes fédéraux doivent être conservées, modifiées ou abrogées. Pour éviter que des vides juridiques ne se forment entre-temps, le P-LPD intègre à l'art. 66 une disposition transitoire qui prévoit que les prescriptions relatives aux données concernant des personnes morales fixées dans des dispositions spéciales de droit fédéral contenues dans une loi au sens formel ou matériel, resteront valables pour les organes fédéraux pendant les cinq ans suivant l'entrée en vigueur du P-LPD. Le but est notamment de permettre aux organes fédéraux de continuer à s'appuyer, s'agissant de la communication de données concernant des personnes morales, sur les bases légales en vigueur pour la communication de données personnelles.

Le projet ne modifie que certaines dispositions spéciales de droit fédéral relatives aux données concernant des personnes morales, pour lesquelles les travaux de révision ont déjà montré qu'une adaptation est nécessaire pour des raisons pratiques et de sécurité juridique. Il s'agit des lois suivantes:

– la LTrans (cf. ch. 9.2.7: art. 3, al. 2, 9, 11, al. 1, 12, al. 2 et 3, et 15, al. 2, let. b);

– la LOGA (cf. ch. 9.2.8: art. 57h^{bis}, 57h^{ter}, 57*i*, 57*j*, 57*k*, phrase introductive, 57*l,* titre et phrase introductive, 57*r*, 57*s*, et 57*t*);

- loi du 16 décembre 2005 sur la surveillance de la révision[193] (cf. ch. 9.2.12: art. 15*b*);
- loi du 9 octobre 1992 sur la statistique fédérale[194] (cf. ch. 9.2.24: art. 5, al. 2, let. a, et 4, let. a, 14, al. 1, 14*a*, al. 1, 15, al. 1, 16, al. 1, et 19, al. 2);
- loi du 17 juin 2005 sur le travail au noir[195] (cf. ch. 9.2.56: art. 17, titre et al. 1 2 et 4, et 17*a*);
- loi du 3 octobre 2003 sur la Banque nationale[196] (cf. ch. 9.2.66: art. 16, al. 5, et 49*a*);
- loi fédérale du 19 mars 1976 sur la coopération au développement et l'aide humanitaire internationales[197] (cf. ch. 9.2.69: art. 13*a*, al. 1);
- loi du 30 septembre 2016 sur l'énergie[198] (cf. ch. 13.7: art. 56, al. 1, 58, titre et al. 1 et 3, et 59, titre et al. 1 et 2) ainsi que la loi sur l'approvisionnement en électricité[199] modifiée par loi du 30 septembre 2016 sur l'énergie (cf. ch. 13.7: art. 17*c*, al. 1, et 27, al. 1).

Art. 67 Disposition transitoire concernant les procédures de certification

En vertu de l'art. 12, al. 2, P-LPD, le Conseil fédéral est tenu d'édicter les dispositions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité. Cette disposition est reprise du droit actuel (art. 11, al. 2, LPD). Il s'agira principalement pour le Conseil fédéral de mettre à jour les textes qu'il a adoptés jusqu'ici, soit notamment l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données[200] et l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation[201]. Compte tenu du caractère technique de ces ordonnances et du peu de temps à disposition pour élaborer l'ensemble des dispositions d'exécution, le Conseil fédéral estime opportun de prévoir un délai transitoire de deux ans. L'ancien droit s'appliquera pendant ce délai.

9.2 Commentaire relatif à la modification d'autres lois fédérales

L'abrogation et la modification d'autres lois fédérales sont réglées dans l'annexe au P-LPD. Ces modifications sont une conséquence du P-LPD.

193 RS **221.302**
194 RS **431.01**
195 RS **822.41**
196 RS **951.11**
197 RS **974.0**
198 FF **2016** 7469
199 RS **734.7**, cf. FF **2016** 7469.
200 RS **235.13**
201 RS **946.512**

9.2.1 Abrogation de la loi du 19 juin 1992 sur la protection des données

Comme le P-LPD est une révision totale de la LPD, cette dernière doit être abrogée.

9.2.2 Modification de la terminologie dans certaines lois fédérales

En raison de la suppression de la notion de «fichier» dans le P-LPD, les lois fédérales spéciales qui recourent à ce terme doivent être adaptées. Par ailleurs, la notion de «maître du fichier» est remplacée par celle de «responsable du traitement».

Le P-LPD abroge la notion de «profils de la personnalité» et introduit celle de «profilage». Comme indiqué au commentaire de l'art. 4, let. f, P-LPD, ces deux notions ne se recoupent pas entièrement, le profilage impliquant une évaluation de certaines caractéristiques d'une personne sur la base d'un traitement de données personnelles automatisé, notamment au moyen d'algorithmes.

L'abrogation de la notion de «profils de la personnalité» implique que les bases légales prévues par un certain nombre de lois fédérales et qui habilitent les organes fédéraux à traiter des profils de la personnalité doivent être adaptées.

Dans un certain nombre de lois fédérales, il suffit de supprimer purement et simplement la référence au profil de la personnalité. Il s'avère en effet que, dans certains domaines, les bases légales habilitant les organes fédéraux à établir des profils de la personnalité n'ont jamais été appliquées. Dans d'autres lois – qui sont commentées ci-après – la notion de «profils de personnalité» doit être soit remplacée par celle de «profilage» (art. 30, al. 2, let. b, P-LPD) soit modifiée en tenant compte de la nouvelle exigence prévue à l'art. 30, al. 2, let. c, P-LPD.

9.2.3 Loi fédérale du 16 décembre 2005 sur les étrangers[202]

Art. 101

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 105, al. 1

En vertu de cette disposition, des données personnelles peuvent être communiqués à l'étranger pour autant que l'Etat ou l'organisation en question garantisse une protection des données équivalente à celle de la Suisse. Les conditions applicables à de telles communications doivent être uniformes en droit fédéral. Il y a lieu par conséquent de prévoir un renvoi à l'art. 13 P-LPD.

202 RS **142.20**

Art. 104, al. 4

Le renvoi au P-LPD est adapté.

Art. 111d, al. 1 et 2

Cette disposition régit la communication de données personnelles dans le cadre des accords d'association à Schengen. L'al. 1 règle la communication des données personnelles aux autorités compétentes d'un Etat tiers en prévoyant un renvoi aux art. 13 et 14 P-LPD. Les modifications apportées aux exceptions prévues à l'al. 2 tiennent compte de la nouvelle teneur de l'art. 14, al, 1, let. a, c et d P-LPD.

Art. 111f, 2e phrase

Cette disposition peut être abrogée au motif que l'obligation pour le responsable du traitement de communiquer à la personne concernée les informations disponibles sur l'origine des données est prévue à l'art. 23, al. 2, let. e, P-LPD.

9.2.4 Loi du 26 juin 1998 sur l'asile[203]

Art. 96, al. 1, 99a, al. 2, let. a, 100, al. 2, et 102, al. 1, 3e phrase, et 2

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 98, al. 1

Voir le commentaire de l'art. 105 P-LEtr du ch. 9.2.3.

Art. 99, al. 6

La notion de maître du fichier est remplacée par celle de «responsable du traitement» et le renvoi au P-LPD, actualisé.

Art. 102c, al. 1 et 2

Voir le commentaire de l'art. 111*d*, al. 1 et 2, P-LEtr (ch. 9.2.3).

Art. 102e, 2e phrase

Voir le commentaire de l'art. 111*f*, 2e phrase, P-LEtr (ch. 9.2.3).

[203] RS **142.31**

9.2.5 Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile[204]

Art. 4, al. 2

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 6 et 7, al. 2

Les renvois au P-LPD sont adaptés.

Art. 15 Communication de données à l'étranger

Il s'agit d'adapter le renvoi de cette disposition aux art. 13 et 14 P-LPD.

Art. 16 Devoir de surveillance des autorités cantonales de protection des données

Cette disposition doit être modifiée en raison de l'abrogation de l'art. 37 LPD.

9.2.6 Loi fédérale du 26 juin 1998 sur l'archivage[205]

Art. 11, al. 1

La notion de «profil de la personnalité» est supprimée pour les motifs exposés sous ch. 9.2.2. Le délai de protection de 50 ans ne s'applique plus que pour les archives classées selon des noms de personnes et contenant des données personnelles sensibles. Pour les autres données personnelles, le délai de protection est de 30 ans.

Art. 15, titre et al. 1

Cette disposition doit être modifiée. En effet, en ce qui concerne le droit d'accès, la loi sur l'archivage renvoie dans son entier à la LPD. Par le biais de cette modification, le renvoi vaut également pour les prétentions découlant de l'art. 16 P-LPD.

204 RS **142.51**
205 RS **152.1**

9.2.7 Loi du 17 décembre 2004 sur la transparence[206]

Art. 3, al. 2

Modification terminologique ne concernant que l'allemand (le terme de «*persönliche Daten*» est remplacé par celui de «*Personendaten*»).

Art. 9 Protection des données personnelles et des données concernant des personnes morales

Du fait de la suppression, dans le P-LPD, de la protection des données concernant des personnes morales et de la limitation, à l'art. 4, let. a, P-LPD, de la définition des données personnelles aux informations concernant une personne physique identifiée ou identifiable, il faut, par mesure de sécurité juridique, préciser à l'art. 9 P-LTrans (cf. ch. 9.1.11) que les documents officiels contenant des données concernant des personnes morales doivent aussi, dans la mesure du possible, être rendus anonymes avant leur consultation (*al. 1*). Il faut aussi préciser le renvoi contenu à l'*al. 2*, dans la mesure où les demandes d'accès à des documents non anonymisés doivent être examinées conformément à l'art. 32 P-LPD, pour ce qui est des données personnelles, et à l'art. 57*s* P-LOGA, pour ce qui est des données de personnes morales.

Art. 11 Droit d'être entendu

L'art. 11, al. 1, LTrans prescrit que la personne concernée doit être consultée lorsque l'autorité envisage d'accorder l'accès à un document officiel contenant des données personnelles. Vu le nouveau champ d'application du P-LPD, le devoir de consulter imposé aux autorités n'est plus assuré. Il est donc nécessaire de modifier l'art. 11, al. 1, LTrans afin de garantir le droit d'être entendu des personnes morales lorsque l'autorité envisage d'accorder l'accès en vertu de l'art. 7, al. 2, LTrans (voir aussi ch. 9.1.11).

La nouvelle teneur de l'*al. 1* réaffirme que l'autorité est tenue de consulter les tiers concernés lorsqu'elle envisage d'accorder l'accès à un document officiel dont la publication est susceptible de porter atteinte à la sphère privée de ces tiers. La notion de sphère privée s'appliquant également aux personnes morales, l'autorité sera tenue de les consulter si elle envisage d'accorder l'accès à un document officiel susceptible de porter atteinte à leur sphère privée (par ex. leur réputation).

La restriction de l'obligation de consulter aux cas dans lesquels l'accès aux données figurant sur un document officiel est susceptible de porter atteinte à la sphère privée des tiers concernés s'applique également aux personnes physiques. Cette disposition tient compte de la jurisprudence du Tribunal fédéral, selon laquelle l'autorité peut s'abstenir de consulter des tiers lorsqu'il n'existe manifestement aucun risque que l'accès aux données personnelles porte atteinte à la sphère privée des personnes concernées[207].

La modification de l'*al. 2* est de nature purement rédactionnelle.

206 RS **152.3**
207 Cf. arrêt du Tribunal fédéral 1C_50/2015 du 2 décembre 2015, consid. 6.3.

Art. 12, al. 2, 2e phrase, et 3

Vu la modification apportée à l'art. 11, al. 1, P-LTrans, il est nécessaire de modifier les al. 2, 2e phrase, et 3 de l'art. 12 pour les rendre applicables aux documents officiels qui, s'ils sont accessibles, risquent de porter atteinte à la sphère privée de tiers.

Art. 15, al. 2, let. b

Pour les raisons exposés ci-dessus, il est nécessaire de compléter l'art. 15, al. 2, let. b, en précisant que l'autorité doit rendre une décision si, en dérogation à la recommandation du préposé, elle entend accorder l'accès à un document officiel alors que cela est susceptible de porter atteinte à la sphère privée de tiers.

Art. 18, phrase introductive

Le renvoi au P-LPD est adapté.

9.2.8 Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[208]

Remarques préalables concernant les art. 57h à 57hter

Contexte: Bases légales des systèmes de gestion des affaires

L'art. 57*h* LOGA constitue la base légale au sens formel pour les systèmes GEVER des diverses unités de l'administration. Le Conseil fédéral a édicté l'ordonnance GEVER du 30 novembre 2012[209] en se fondant sur l'al. 3 de cet article.

Acta Nova, le nouveau système GEVER de l'administration fédérale, développé en ce moment, et qui sera utilisé par l'ensemble de l'administration fédérale, doit être introduit par étapes d'ici 2020 (programme GENOVA) dans l'administration fédérale centrale et dans certaines unités de l'administration fédérale décentralisée (comme le préposé). Ce nouveau système permettra aux diverses unités administratives d'obtenir l'accès aux systèmes GEVER d'autres unités administratives pour assurer le bon déroulement de processus interdépartementaux (comme les consultations des offices et le traitement des affaires du Conseil fédéral). On pourra ainsi simplifier des processus et éliminer les ruptures de médias. Les dossiers mis en consultation auprès des offices, par exemple, ne devront plus être distribués par courrier électronique. A l'avenir, il suffira d'envoyer un lien vers le dossier correspondant, et les unités administratives invitées à se prononcer pourront travailler directement sur un document de base. Outre ces procédures de consultation, d'autres processus d'affaires concernant plusieurs unités administratives (comme les adjudications, le programme de la législature, les objectifs du Conseil fédéral et le rapport de gestion) pourront être exécutés sur GEVER. La licence acquise à l'issue d'une

208 RS **172.010**
209 RS **172.010.441**

procédure OMC autorise aussi bien l'administration fédérale centrale que l'administration fédérale décentralisée à utiliser le nouveau système GEVER.

En plus des autres unités administratives, il faut que des services cantonaux, communaux ou privés (entreprises, citoyens) puissent obtenir un accès ponctuel et clairement délimité au nouveau système GEVER, dans le cadre de processus de cyberadministration. Pour cette raison, la licence acquise en vue de l'exploitation du nouveau système GEVER autorisera ces accès «de l'extérieur» sans restrictions ni coûts supplémentaires.

Nécessité d'adapter les bases légales

Le message du Conseil fédéral concernant la création et l'adaptation des bases légales nécessaires au traitement de données sensibles ou de profils de la personnalité[210] expose à propos de l'art. 57*h* LOGA ce qui suit: «La disposition proposée ne s'étend toutefois *pas* aux systèmes d'enregistrement utilisés en commun par plusieurs organes fédéraux et qui contiennent des données personnelles auxquelles ces différents organes ont accès. Il est en effet nécessaire de créer une *base légale spécifique* pour ces systèmes, notamment pour régler la communication régulière de données sensibles ou de profils de la personnalité, en particulier par le biais de la procédure d'appel, conformément à l'art. 19, al. 1 et 3, LPD.»

Conformément à l'art. 19, al. 3, 1re phrase, LPD, «les organes fédéraux ne sont en droit de rendre des données personnelles accessibles en ligne que si cela est prévu expressément». Quant à la 2e phrase, elle dispose que «les *données sensibles* ou les *profils de la personnalité* ne peuvent être rendus accessibles en ligne que si une *loi au sens formel* le prévoit expressément». Cette disposition est abrogée par le P-LPD.

Dans le cadre des processus transversaux usuels concernant deux ou plusieurs départements ou unités administratives (procédures de consultation des offices, traitement d'affaires du Conseil fédéral, processus de planification, projets de marchés publics), il est très exceptionnel que des données sensibles soient traitées (en ce qui concerne les affaires du Conseil fédéral, ce sont par ex. les décisions sur recours, les cas dans lesquels la responsabilité de la Confédération est engagée, les décisions et les rapports concernant l'interdiction d'exercer une activité au sens de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure [LMSI][211], la gestion des ressources humaines). *Stricto sensu*, l'art. 17, al. 2, LPD exige que ce type de traitements de données repose également sur une base légale au sens formel. A l'avenir, une ordonnance devrait toutefois suffire si le traitement est indispensable à l'exécution d'une tâche définie dans une loi au sens formel et qu'il n'entraîne pas de risques particuliers pour les droits fondamentaux des personnes concernées (cf. art. 30, al. 3, P-LPD).

En règle générale, la base légale spécifique permettant de traiter des données personnelle doit aujourd'hui déjà découler du droit spécial. L'art. 57*h* LOGA en vigueur ne constitue toutefois que la base légale nécessaire pour rendre accessibles en ligne des données personnelles sensibles, comme le veut la disposition correspondante (qu'il est prévu d'abroger) de l'art. 19, al. 3, LPD.

210 FF **1999** 8381, 8385
211 RS **120**

Comme cet art. 57*h* LOGA est en rapport étroit avec le droit général de la protection des données et qu'il concrétise ce droit dans un domaine important du traitement de données par l'administration fédérale, son adaptation dans le cadre de la révision de la LPD s'impose. Pour des raisons de transparence, le passage fondamental du principe de l'entreposage des données au principe du traitement centré sur des processus dans le cadre des systèmes GEVER devrait être rendu manifeste dans une base légale adaptée en conséquence.

En raison de l'abrogation de la protection des données des personnes morales dans le P-LPD, ainsi que de la limitation de la notion de données personnelles dans l'art. 4, let. a, P-LPD aux informations qui se rapportent à une personne physique identifiée ou identifiable, il doit être clarifié dans les art. 57*h*^{bis} et 57*h*^{ter}, pour des raisons de sécurité du droit, que ces normes s'appliquent aussi aux données des personnes morales (voir les explications sous ch. 9.1.11).

Art. 57h Gestion

Le contenu de l'art. 57*h* en vigueur doit être réparti entre trois articles distincts. Il comprend des dispositions relatives aussi bien à l'exploitation de systèmes de gestion des affaires qu'aux traitements de données personnelles dans ces systèmes. Ces deux aspects doivent être distingués et traités séparément.

Al. 1: La mise en œuvre de systèmes de gestion électronique des affaires (systèmes GEVER) est aujourd'hui impérative pour l'administration fédérale centrale (cf. notamment l'art. 1, al. 1, de l'ordonnance GEVER du 30 novembre 2012[212]). Les systèmes GEVER doivent entre autres permettre de traiter les affaires conformément au droit, sur la base de processus et de manière transparente (art. 1, al. 2, de l'ordonnance GEVER). La disposition prévue doit donc être légèrement étendue par rapport à sa teneur actuelle. Il n'est pas seulement question de gestion des affaires au sens procédural, mais aussi de stockage de documents à plus ou moins long terme (par ex. en vue de l'enregistrement de l'activité de l'administration prévu à l'art. 22 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration[213] et de l'archivage ultérieur). A l'avenir, la fonction documentaire des systèmes GEVER pourra éventuellement être étoffée davantage.

Le système EXE-BRC, qui sert notamment à gérer les affaires du Conseil fédéral, est lui aussi un système de gestion des affaires au sens de la présente disposition.

Les unités de l'administration fédérale auxquelles la disposition s'adresse sont en principe les offices. Le Département fédéral des affaires étrangères (DFAE), en raison

212 RS **172.010.441**. L'art. 1, al. 1, de l'ordonnance GEVER a la teneur suivante: «L'administration fédérale traite en principe au moyen de systèmes de gestion électronique des affaires (systèmes GEVER) les documents importants pour les affaires. Sont considérés comme tels les documents dans lesquels est consignée l'activité de l'administration au sens de l'art. 22 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA).» A ce sujet, voir également les explications du message du Conseil fédéral du 11 septembre 2015 relatif au financement de la réalisation d'un produit GEVER standardisé et de l'introduction de ce produit dans l'administration fédérale centrale, FF **2015** 6357.

213 RS **172.010.1**

de sa structure organisationnelle, ne gère toutefois qu'un seul système GEVER pour l'ensemble du département.

L'*al. 2* prévoit que les unités de l'administration fédérale centrale ou décentralisée responsables d'un système GEVER peuvent donner accès de manière restreinte à leurs systèmes de gestion des affaires à d'autres autorités fédérales (unités de l'administration fédérale centrale ou décentralisée, les Services du Parlement ou les tribunaux fédéraux, par ex.), et à des unités extérieures à l'administration fédérale (services cantonaux ou conférences intercantonales, par ex.). Il s'agit de permettre que certains processus d'affaires, comme la consultation des offices, le traitement des affaires du Conseil fédéral, les adjudications ou les processus de reddition de comptes (voir plus haut), puissent être gérés dans ces systèmes. De plus, la collaboration interdépartementale doit pouvoir être simplifiée.

Il en résultera que l'envoi de documents par courrier électronique sera souvent rendu superflu. En fin de compte, il sera possible de mieux protéger les processus et les informations correspondantes contre les accès non autorisés.

*Art. 57h^bis^* Traitement de données personnelles et de données concernant des personnes morales

L'al. *1* correspond pour l'essentiel à l'actuel art. 57*h*, al. 1, dernière phrase, LOGA. Cette disposition énonce les buts en vue desquels le traitement de données personnelles et les données concernant des personnes morales dans un système de gestion des affaires est licite. Cette concrétisation, nécessaire au regard du droit de la protection des données, est ainsi maintenue. Elle découle des art. 4, al. 3, et 17, al. 1, LPD (cf. art. 5, al. 3 et 30, al. 1, P-LPD). La base légale pour le traitement (particulièrement la collecte et la communication) de données personnelles et de données concernant des personnes morales doit néanmoins toujours découler du droit spécial applicable aux données en question. La présente disposition autorise le traitement dans la perspective du bon déroulement des processus opérationnels.

La nécessité de disposer d'une base légale pour pouvoir communiquer des données personnelles, qui figure explicitement à l'*al. 2*, établit clairement que cette base légale doit figurer dans le droit spécial. Si tel est le cas, il est possible d'autoriser un accès (restreint de manière appropriée) au système GEVER de l'unité administrative responsable au premier chef.

L'*al. 3* correspond à l'actuel art. 57*h*, al. 1, 2e phrase, LOGA. La disposition est légèrement adaptée sur le plan rédactionnel. La révision supprime la notion de «profil de la personnalité»; cette suppression doit se refléter ici. En raison de l'abrogation de la protection des données des personnes morales dans le P-LPD, il doit être prévu expressément que le système de gestion des affaires peut également contenir des données sensibles concernant des personnes morales, c'est-à-dire des données sur des poursuites et des sanctions administratives ou pénales ainsi que des secrets professionnels, d'affaires ou de fabrication (cf. art. 57*r*, al. 2, P-LOGA ainsi que les explications au ch. 9.1.11).

Al. 4: En soi, cette disposition est de nature déclaratoire. Le principe selon lequel l'accès doit être restreint découle directement du principe de la proportionnalité (art. 5, al. 2, Cst. et art. 4, al. 2, LPD resp. 5, al. 2, P-LPD). C'est à l'organe fédéral

responsable du système qu'il incombe de circonscrire cet accès. La formulation de l'actuel art. 57*h*, al. 2, LOGA, qui précise que l'accès est limité aux «seuls» collaborateurs de l'organe concerné, est cependant inadéquate. Les possibilités d'accès nécessaires au bon déroulement des processus exigeront régulièrement un accès «depuis l'extérieur» à des métadonnées, par exemple, qui peuvent contenir des données comme les noms, numéros de téléphone et adresses électroniques de collaborateurs de l'administration.

Les futurs systèmes GEVER permettent de régler les accès d'après la fonction exercée par le bénéficiaire de l'accès et de chiffrer systématiquement les données; ils offrent donc suffisamment de possibilités pour que la présente disposition puisse être mise en oeuvre. Les modalités seront à régler à l'échelon réglementaire (cf. les actuels art. 6 ss de l'ordonnance GEVER). Il conviendra également de régler, le cas échéant, les exigences en matière de sécurité auxquelles les personnes et les organisations extérieures à l'administration fédérale auront à satisfaire pour pouvoir bénéficier d'un accès au système.

*Art. 57h^ter^* Dispositions d'exécution

L'art. 57*h^ter^* correspond pour l'essentiel à l'actuel art. 57*h*, al. 3, LOGA. La délégation de compétence prévoit également le droit d'établir des règles particulières concernant les directives applicables aux systèmes exploités par les unités de l'administration fédérale décentralisée.

Avec la nouvelle licence Acta Nova, la Confédération a entre-temps acquis le droit d'équiper également du nouveau système GEVER les unités de l'administration fédérale décentralisée, sans devoir s'acquitter de coûts de licence supplémentaires. A moyen et à long terme, on peut donc s'attendre à ce que ces unités travaillent elles aussi avec la norme fédérale, pour s'épargner des coûts et simplifier la collaboration électronique entre unités administratives.

Art. 57i Relation avec d'autres lois fédérales

Pour des motifs de sécurité juridique, l'art. 57*i* prévoit que les dispositions de la section 2 ne sont pas applicables lorsqu'une autre loi fédérale règle le traitement de données liées à l'utilisation d'un infrastructre électronique, qu'il s'agisse de données personnelles ou de données concernant des personnes morales (cf. ch. 9.1.11).

Art. 57j Principes

Du fait de la suppression, dans le P-LPD, de la protection des données concernant des personnes morales et de la limitation, à l'art. 4, let. a, P-LPD, de la définition des données personnelles aux informations concernant une personne physique identifiée ou identifiable, il faut, par mesure de sécurité juridique, préciser à l'art. 57*j*, al. 1 et 2, que ces dispositions s'appliquent aux données concernant des personnes morales (cf. ch. 9.1.11). Les données sensibles concernant des personnes morales comprennent les données relatives à des poursuites et des sanctions administratives ou pénales, ou encore des secrets professionnels, d'affaires ou de fabrication (cf. art. 57*r*, al. 2).

La notion de «profil de la personnalité» est par ailleurs supprimée de l'al. 2. Voir le commentaire du ch. 9.2.2.

Art. 57k, phrase introductive

Le terme «données personnelles» est complété par le terme «données concernant des personnes morales». Voir les commentaires qui précèdent et le ch. 9.1.11.

Art. 57l, titre et phrase introductive et let. b, ch. 4

Dans le titre et dans la phrase introductive, le terme «données personnelles» est complété par le terme «données concernant des personnes morales». Voir les commentaires qui précèdent et le ch. 9.1.11.

La notion de «fichier» à la let. b, ch. 4, est remplacée par celle d'«infrastructure». Voir le commentaire du ch. 9.2.2.

Art. 57r Traitement de données concernant des personnes morales

En raison de l'abrogation de la protection des données personnelles des personnes morales, les bases légales prévues par le droit fédéral qui habilitent les organes fédéraux à traiter des données personnelles ne s'appliquent plus lorsque ceux-ci traitent des données concernant des personnes morales. Or l'art. 5 Cst. exige que l'activité de l'Etat soit régie par la loi. De plus, toute tâche d'un organe fédéral susceptible de porter atteinte à la sphère privée d'une personne morale (art. 13 Cst.) ou de restreindre sa liberté économique (art. 27 Cst.) doit respecter les exigences de l'art. 36 Cst. (exigence d'une base légale, existence d'un intérêt public prépondérant et respect du principe de la proportionnalité). Le Conseil fédéral considère par conséquent qu'il est nécessaire de créer une base légale générale qui habilite les organes fédéraux à traiter des données concernant des personnes morales, y compris de données sensibles, dans la mesure où l'accomplissement de leurs tâches l'exige et que celles-ci sont définies dans une loi au sens formel (*al. 1*). La notion d'«organes fédéraux» se réfère à la définition légale de l'art. 4, let. h, P-LPD; l'administration décentralisée entre aussi dans cette notion.

A l'*al. 2*, la disposition définit la notion de données sensibles pour les personnes morales. Elle se réfère aux données sur des poursuites ou des sanctions administratives ou pénales (*let. a*) ou sur les secrets professionnels, d'affaires ou de fabrication (*let. b*).

Art. 57s Communication de données concernant des personnes morales

Al. 1 Communication de données concernant des personnes morales

Cette disposition pose le principe que les organes fédéraux ne peuvent communiquer des données concernant des personnes morales que si une base légale le prévoit. Celle-ci peut être prévue par un traité international, une loi au sens formel ou par une ordonnance. Ce principe général correspond à celui prévu à l'art. 32, al. 1, P-LPD relatif à la communication de données personnelles.

Al. 2 Exigence d'une base légale au sens formel

Cette disposition prévoit que les organes fédéraux ne sont en droit de communiquer des données sensibles concernant des personnes morales (c'est-à-dire des données concernant des poursuites ou des sanctions pénales et administratives ou des secrets professionnels, d'affaires ou de fabrication) que si une base légale prévue dans une loi au sens formel le prévoit. La communication de telles informations peut en effet constituer une restriction grave, au sens de l'art. 36, al. 1, 2e phrase, Cst., aux droits fondamentaux d'une personne morale. Une base légale au sens formel est donc nécessaire.

Al. 3 Dérogations

L'al. 3 prévoit une dérogation à l'exigence d'une base légale au sens de l'al. 1 et 2 si l'une des conditions prévues aux *let. a* à *c* est réalisée. Cette disposition correspond aux exceptions prévue par l'art. 32, al. 2, let. a, b et e, P-LPD.

Les *al. 4* à *6* correspondent à la réglementation prévue à l'art. 32, al. 3, 5 et 6, P-LPD.

Art. 57t Droits des personnes morales

Au lieu d'introduire expressément un droit d'accès ou de rectification, qui relève typiquement de la législation sur la protection des données, le Conseil fédéral est d'avis que le droit de procédure applicable constitue une réglementation suffisante pour garantir les droits des personnes morales découlant de l'art. 13, al. 2, Cst. Ainsi, dans la cadre d'une procédure administrative de première instance, celles-ci peuvent consulter les pièces conformément aux art. 26 ss PA, exercer le droit d'être entendu selon les art. 29 ss PA et recourir, le cas échéant, contre la décision rendue par l'autorité compétente. Enfin, les personnes morales peuvent également se prévaloir de l'art. 25*a* PA. Selon cette disposition, toute personne qui a un intérêt digne de protection peut exiger que l'autorité compétente pour des actes fondés sur le droit public fédéral et touchant à des droits ou des obligations rende une décision susceptible de recours en ce qui concerne des actes matériels illicites. Ce faisant, les personnes morales peuvent obtenir le droit de faire rectifier des données les concernant, voire de les faire détruire.

9.2.9 Loi du 24 mars 2000 sur le personnel de la Confédération[214]

Art. 27, al. 2, phrase introductive et let. b

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Il convient de signaler que l'art. 27 LPers a été modifié dans le cadre de la révision du 16 juin 2017 de la loi sur les fonds de compensation[215]. Lors de l'élaboration des

214 RS **172.220.1**

normes de coordination à la fin de la procédure parlementaire (cf. ch. 13.7), il s'agira de tenir compte de la nouvelle teneur de cette disposition et de supprimer la notion de «profils de la personnalité».

Art. 27d, al. 2, phrase introductive, et 4, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.10 Loi du 17 juin 2005 sur le Tribunal administratif fédéral[216]

Art. 35, let. b

Cette disposition peut être abrogée puisque le P-LPD confère des compétences décisionnelles au préposé (art. 44 et 45 P-LPD).

9.2.11 Code civil[217]

Art. 45a, al. 3, ch. 3

L'art. 45*a*, al. 3, ch. 3, P-CC[218] charge le Conseil fédéral de régler, avec le concours des cantons, la surveillance du registre informatisé de l'état civil. Il s'agit en particulier de modifier l'art. 83 de l'ordonnance du 28 avril 2004 sur l'état civil[219], en s'inspirant par exemple de la solution prévue à l'art. 55, al. 1, de l'ordonnance N-SIS du 8 mars 2013[220], qui prescrit que les autorités cantonales de protection des données et le préposé collaborent activement dans le cadre de leurs compétences respectives et veillent à exercer une surveillance coordonnée du traitement de données personnelles. Par rapport à la surveillance du registre informatisé de l'état civil, le préposé et les autorités cantonales de protection des données ne doivent pas empiéter sur la compétence de la justice de modifier les données litigieuses (art. 42 CC).

Il convient de signaler que l'art. 45*a* CC est modifié dans le cadre du projet de révision du Conseil fédéral du 16 avril 2014[221]. Lors de l'élaboration des normes de coordination à la fin de la procédure parlementaire (cf. ch. 13.7), il s'agira de tenir compte de la nouvelle teneur de cette disposition et de procéder aux adaptations nécessaires.

215 FF **2017** 3957
216 RS **173.32**
217 RS **210**
218 Cf. message du Conseil fédéral du 16 avril 2014 concernant la modification du code civil (Enregistrement de l'état civil et registre foncier), FF **2014** 3395.
219 RS **211.112.2**
220 RS **362.0**
221 FF **2014** 3439

9.2.12 Loi du 16 décembre 2005 sur la surveillance de la révision[222]

Art. 15b Traitement de données personnelles et de données concernant des personnes morales

Dans le cadre de l'exécution de ses tâches légales, l'Autorité fédérale de surveillance en matière de révision (ASR) traite une multitude de données concernant des personnes physiques et morales. Elle collecte ces données dans le cadre des devoirs légaux de renseignement et de communication (art. 15*a* de la loi sur la surveillance de la révision [LSR]), dans le cadre de son contrôle (art. 16 LSR) et dans le cadre de l'assistance administrative (art. 22 ss LSR). A ces données appartiennent des données générales comme des données de contact ou d'identification d'un requérant ou du détenteur d'autorisation, mais également des données pertinentes pour l'autorisation et la surveillance, par exemple sur la formation et le parcours professionnel, l'extrait du casier judiciaire, des données en rapport avec des procédures pénales ou de droit pénal administratif et des procédures en responsabilité civile ou administrative ou des informations sur l'organisation et l'activité de l'entreprise de révision et sur l'exercice du service de révision. Par mesure de sécurité juridique, l'art. 15*b* P-LSR précise que l'ASR peut, afin d'accomplir ses tâches légales, traiter les données personnelles et les données concernant des personnes morales, y compris les données sensibles. Les données sensibles concernant des personnes morales comprennent notamment les données relatives à des poursuites et des sanctions administratives ou pénales, ou encore des secrets professionnels, d'affaires ou de fabrication (voir aussi ch. 9.2.8).

9.2.13 Loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères[223]

Art. 1, 2e phrase

Cette disposition est superflue. Elle peut donc être abrogée.

Art. 2, al. 1 et 2, 1re phrase

En raison de l'abrogation de la notion de «fichier», l'al. 1 doit être modifié. La base légale habilitant les services compétents du DFAE à traiter des données personnelles reste néanmoins la même.

L'al. 2 subit deux modifications. Il s'agit d'abord de supprimer la notion de «fichier». Il s'agit ensuite de remplacer la notion de «profils de la personnalité» par celle de «données personnelles en vue d'évaluer l'aptitude des personnes concernées à assumer un engagement au sens de l'al. 1».

222 RS **221.302**
223 RS **235.2**

Art. 5, al. 1, phrase introductive, et 3

La notion de «fichier» est supprimée. Voir le commentaire du ch. 9.2.2. Dans la version allemande, la notion «*administrative und strafrechtliche Massnahmen*» est adaptée à la terminologie de l'art. 4, let. c, ch. 5, P-LPD.

Art. 6, let. a

La notion de «fichier» est supprimée. Voir le commentaire du ch. 9.2.2.

Il convient de signaler que la loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères est en cours de révision. La consultation externe concernant l'avant-projet de révision du Conseil fédéral du 28 juin 2017 se termine le 20 octobre 2017. Il s'agira le cas échéant d'adapter certains termes de cette loi à la nouvelle terminologie de la future LPD.

9.2.14 Loi fédérale du 19 décembre 1986 contre la concurrence déloyale[224]

Art. 22, al. 2, 2e phrase

Le renvoi à l'art. 6 LPD doit être adapté à la nouvelle numérotation du P-LPD (art. 13 et 14).

9.2.15 Code de procédure civile[225]

Les modifications du code de procédure civile (CPC) proposées ont été de manière générale bien accueillies lors de la consultation.

Art. 20, let. d: For

L'art. 20 CPC règle dorénavant le for de l'ensemble des actions civiles en matière de protection des données. Il s'agit notamment des actions en exécution du droit à la consultation et à l'effacement selon l'art. 16 P-LPD, du droit d'accès selon l'art. 23 P-LPD et des différentes actions de l'art. 28 P-LPD.

Suppression des frais de justice

L'évaluation de la LPD a montré que les personnes concernées sont peu enclines à exercer leurs droits, voire à les faire valoir en justice, en particulier dans le secteur privé[226], en raison notamment du risque de devoir supporter les coûts de procédure. L'efficacité de la LPD s'en trouve considérablement réduite. Par ailleurs, il manque

224 RS **241**
225 RS **272**
226 Cf. pp. 90 ss et 219 du rapport intitulé «Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz vom 10. März 2011» (disponible uniquement en allemand).

une jurisprudence claire en matière de protection des données, qui concrétiserait les normes et offrirait une meilleure sécurité juridique.

Afin de simplifier la mise en œuvre procédurale des droits des personnes concernées, il est prévu comme mesure principale de supprimer les frais de justice pour les actions civiles relevant de la protection des données. Cette mesure existe déjà pour d'autres procédures et domaines du droit (par ex. pour les procédures découlant de la loi sur l'égalité, en matière de droit du travail jusqu'à une valeur litigieuse de 30 000 francs, ou pour les litiges relevant de la loi du 17 décembre 1993 sur la participation[227]). Le risque financier pour les personnes concernées sera ainsi réduit sur un point important. Comme la majorité des prétentions de droit de la protection des données ne sont pas de nature financière, il ne semble pas opportun de fixer une valeur litigieuse limite, comme dans le droit du travail. Vu le petit nombre de cas portés devant les tribunaux jusqu'ici, il est peu probable que cette modification entraîne une augmentation considérable ou favorise des demandes irréfléchies. La partie qui succombe devra en effet toujours verser des dépens et assumer elle-même ses frais de représentation, et des frais judiciaires pourront tout de même lui être imputés si elle a procédé de façon téméraire ou de mauvaise foi (art. 115 CPC).

Art. 99, al. 3, let. d

L'art. 99, al. 1, CPC prévoit l'obligation pour le demandeur de fournir des sûretés en garantie du paiement des dépens, sur demande de la partie défenderesse. Cette obligation est supprimée pour les procédures relevant de la LPD. La charge financière de la partie demanderesse est ainsi réduite.

Cette suppression concerne les actions civiles au sens de l'art. 28 P-LPD qui relèvent de la procédure ordinaire. Elle vise à faciliter de telles actions, qui n'ont été que rarement intentées jusqu'à présent. Les personnes qui introduisent une action relevant de la procédure simplifiée au sens de l'art. 243, al. 2, let. d, CPC sont déjà exemptées de l'obligation de fournir des sûretés (cf. art. 99, al. 3, CPC). Cela ne va pas changer.

Art. 113, al. 2, let. g

Le CPC est complété de sorte que des frais judiciaires ne soient plus perçus pour les procédures de conciliation concernant la LPD, qui sont en principe obligatoires aussi bien dans la procédure ordinaire que dans la procédure simplifiée (art. 197 CPC). Une telle exemption est déjà prévue pour les litiges portant par exemple sur des baux à loyer ou à ferme d'habitation ou de locaux commerciaux ou ceux relevant de la loi sur la participation (cf. art. 113, al. 2, CPC).

L'exemption des frais judiciaires réduit le risque financier encouru par la personne concernée pour toutes les actions civiles en matière de protection des données. Cela est d'autant plus déterminant qu'il n'est en principe pas alloué de dépens en procédure de conciliation (cf. art. 113, al. 1, 1re phrase, CPC). Le requérant doit en principe assumer ses frais de représentation, à moins de bénéficier de l'assistance judiciaire.

227 RS **822.14**

Art. 114, let. f

Le CPC est complété de manière que, dans la procédure au fond, il n'est pas perçu de frais judiciaires pour les litiges relevant de la LPD, à l'instar de ce qui est prévu pour les litiges relevant de la loi sur l'égalité ou de la loi sur la participation et pour les litiges de droit du travail dont la valeur litigieuse s'élève à 30 000 francs au plus.

La nouvelle règle réduit le risque financier pour la personne concernée. Les dépens continuent en revanche d'être répartis selon les normes usuelles (cf. art. 104 ss CPC).

Art. 243, al. 2, let. d: Type de procédure

Les actions fondées sur l'art. 16 P-LPD sont soumises à la procédure simplifiée, comme les actions en exécution du droit d'accès. Cette modification est nécessaire dans la mesure où l'art. 16 est nouveau.

Art. 407d (Disposition transitoire)

Les nouvelles règles de procédure s'appliqueront, dès l'entrée en vigueur, à toutes les procédures, y compris celles qui sont pendantes. En particulier, une sûreté ne devra plus être fournie et le paiement de frais judiciaires ne pourra plus être prononcé (art. 113, al. 2, let. g, et art. 114, let. f, P-CPC).

9.2.16 Loi fédérale du 18 décembre 1987 sur le droit international privé[228]

Art. 130, al. 3

Comme indiqué plus haut (cf. ch. 9.2.2) l'évolution technologique rend la notion de «fichier» dépassée. De plus, cette notion n'est guère utilisée dans les systèmes juridiques d'autres Etats. Le P-LPD n'utilise plus, lui aussi, que la notion de «traitement des données». Il semble dès lors approprié de modifier également l'art. 130, al. 3, LDIP, qui fait mention du «lieu où le fichier est géré ou utilisé».

L'art. 130 P-LDIP continue de prévoir que les actions en exécution du droit d'accès ou de consultation par rapport à un traitement de données personnelles peuvent être intentées devant les tribunaux mentionnés à l'art. 129 LDIP. La personne concernée peut ainsi intenter action en Suisse à son gré aux lieux suivants: au lieu du domicile ou, à défaut, au lieu de la résidence habituelle de la personne responsable, au lieu de l'établissement de la personne responsable ou encore au lieu de l'acte ou du résultat. L'acte illicite au sens de l'art. 129 LDIP consiste en l'espèce dans le refus d'accorder un droit d'accès ou de consultation existant. Le lieu de l'acte est ainsi le lieu où le droit d'accès ou de consultation aurait dû être exercé[229]. C'est en règle générale le lieu où la personne responsable exerce l'activité dans le cadre de laquelle le traitement de données en cause s'opère. Le lieu du résultat est le lieu où la

228 RS **291**

229 Cf. ATF **113** II 476, consid. 3, et **125** III 346, consid. 4c/bb, concernant le lieu de l'acte en cas d'omission.

personne concernée aurait dû pouvoir exercer son droit d'accès ou de consultation. C'est en règle générale le lieu de sa résidence habituelle[230].

Contrairement à l'avant-projet mis en consultation, il n'est plus fait mention du second terme de l'alternative, qui prévoyait d'intenter action au «lieu où les données personnelles sont traitées» (ce passage devait remplacer le terme existant d'intenter action au «lieu où le fichier est géré ou utilisé»). On peut partir du principe qu'un droit d'accès ou de consultation fondé sur un droit étranger se dirige également contre la personne qui est responsable du traitement des données (cf. art. 15 du règlement [UE] 2016/679). Il serait dès lors indiqué ici de considérer comme lieu du traitement des données le lieu où la personne concernée exerce l'activité dans le cadre de laquelle le traitement des données en cause s'opère[231]. Ceci correspond au lieu de l'acte déjà mentionné à l'art. 129, al. 1, LDIP (cf. paragraphe précédent). Il conviendrait également en règle générale d'y assimiler le lieu de l'établissement de la personne concernée[232], qui figure également à l'art. 129, al. 1, LDIP. Pour certains auteurs, le for au lieu du traitement des données découle même directement du lieu du résultat de l'art. 129, al. 1, LDIP[233]. Dans ce contexte, le passage supprimé n'aurait amené aucun avantage et aurait au contraire seulement prêté à confusion.

Dans le cadre de la procédure de consultation externe, quelques participants ont proposé de compléter l'art. 139, al. 3, LDIP par une nouvelle phrase. La disposition actuelle prévoit que l'art. 139, al. 1, LDIP, qui règle le droit applicable aux atteintes à la personnalité, «s'applique également aux atteintes à la personnalité résultant du traitement de données personnelles ainsi qu'aux entraves mises à l'exercice du droit d'accès aux données personnelles». La phrase complémentaire proposée aurait par exemple la teneur suivante: «Le lieu à l'étranger du résultat de l'atteinte au sens de l'al. 1, let. c, ne peut pas se fonder uniquement sur le fait que les données sont enregistrées dans l'Etat correspondant». Le Conseil fédéral renonce à une telle modification car il la juge inutile. Le lieu du résultat au sens de l'art. 139, al. 1, let. c, est en effet à déterminer en lien avec l'atteinte alléguée. Le seul lieu d'enregistrement des données ne peut entrer en ligne de compte comme lieu du résultat que dans des cas très spécifiques, comme lorsqu'il est fait valoir que la manière d'enregistrer les données contrevient à des normes de protection des données[234]. On ne peut donc jamais fonder le lieu du résultat au sens de l'art. 139, al. 1, let. c, LDIP uniquement sur le fait que les données sont enregistrées dans l'Etat concerné. Au vu de ce qui

230 Cf. Rosenthal David, in: Rosenthal David/Jöhri Yvonne (édit.), Handkommentar zum Datenschutzgesetz, Zurich 2008, art. 139 LDIP nº 24; même conclusion chez Vischer Frank, in: ZK-IPRG, 2e édit., Zurich 2004, art. 139 LDIP nº 28; Umbricht Robert/Rodriguez Rodrigo/Krüsi Melanie, in: Honsell Heinrich/Vogt Nedim Peter, Schnyder Anton K./Berti Stephen V. (édit.), BSK-IPRG, 3. A., Bâle 2013, art. 130 LDIP nº 11, et Bonomi Andrea, in: Bucher Andreas (édit.), CR-LDIP/CL, art. 139 LDIP nº 16; dans le cas présent, on pourrait aussi opérer un rattachement avec le domicile habituel de la personne concernée, comme le fait Dasser Felix, in: BSK-IPRG, avec renvois, art. 139 LDIP nº 43.

231 Cf. Dasser, in: BSK-IPRG, avec renvois, art. 139 LDIP nº 45.

232 Cf. «La responsabilité civile des fournisseurs de services Internet», rapport du Conseil fédéral du 11 décembre 2015, pp. 90 ss.

233 Par ex. Bucher Andreas, Le premier amendement de la LDIP, in: Etudes de droit international en l'honneur de Pierre Lalive, Bâle 1993, p. 8.

234 Cf. ROSENTHAL, Handkommentar zum Datenschutzgesetz, avec renvois, art. 139 LDIP nº 22.

précède, il est très peu probable que le droit du simple lieu d'enregistrement de données soit appliqué dans le cadre d'actions en exécution d'un droit d'accès ou de consultation.

9.2.17 Code pénal[235]

Art. 179novies Soustraction de données personnelles

Cette disposition ne s'appliquera plus aux données de personnes morales, ces dernières n'étant plus soumises à la protection de la loi. La disposition transitoire de l'art. 66 P-LPD ne s'applique pas. Les références au profil de la personnalité et au fichier sont par ailleurs supprimées, pour faire suite à l'abrogation de ces notions dans le P-LPD. Enfin, la disposition remplace l'expression «qui ne sont pas librement accessibles» par «qui ne sont pas accessibles à tout un chacun».

Art. 179decies Usurpation d'identité

La motion Comte (14.3288), adoptée par le Parlement, charge le Conseil fédéral d'élaborer un projet de modification du code pénal, afin que l'usurpation d'identité, qui constitue une grave atteinte à la personnalité, soit considérée comme une infraction en soi.

L'identité d'une personne peut être déterminée au moyen de différents éléments, comme son nom, son origine, sa photo, son statut social, familial ou professionnel ou d'autres données personnelles encore, comme sa date de naissance, son adresse Internet, son numéro de compte ou son nom d'utilisateur.

La disposition pénale proposée contre l'usurpation d'identité protège la personnalité, à savoir le droit de la personne au respect de son identité, et punit toute usurpation de cette identité en tant qu'élément de la personnalité. D'un point de vue systématique, la norme s'insère sous le titre «Infractions contre l'honneur et contre le domaine secret ou le domaine privé»[236]. Il n'est pas question de punir le fait de s'affubler de l'identité d'un tiers dans un élan d'exubérance ou d'espièglerie, ni celui d'utiliser une identité inventée. Cela serait disproportionné d'un point de vue pénal. La disposition ne doit s'appliquer qu'à l'auteur qui agit dans l'intention de causer un dommage ou d'obtenir un avantage.

Le phénomène et la problématique de l'usurpation d'identité ont gagné en acuité en raison de la diffusion des moyens de communication électronique et de l'utilisation des médias sociaux. La limite qui retient un individu de tenir des propos ou de commettre des actes au nom d'un autre s'est considérablement abaissée par rapport aux anciens médias. La disposition pénale proposée n'est cependant pas liée au média ou moyen de communication utilisé pour commettre l'acte. Elle sanctionne aussi l'auteur qui a par exemple commandé par écrit une marchandise ou qui a pris des renseignements auprès d'une personne âgée pour se faire passer ensuite au

235 RS **311.0**
236 Art. 173 ss CP

téléphone pour un de ses petits-enfants. La disposition ne s'applique donc pas uniquement aux usurpateurs qui utilisent un ordinateur ou un téléphone.

La nuisance causée par l'usurpation d'identité peut être de nature matérielle ou immatérielle et doit atteindre un certain degré pour que la disposition s'applique. La seule intention de causer de graves ennuis peut déjà être considérée comme une nuisance suffisante[237].

Lorsque l'usurpation d'identité a pour but de causer une nuisance ou d'obtenir un avantage illicite, il y a lieu de se demander si d'autres dispositions pénales ne s'appliquent pas (par ex. escroquerie, faux dans les titres ou infraction contre l'honneur). Dans les cas où le bien juridique touché (l'atteinte à la personnalité) ne coïncide pas entièrement avec les faits constitutifs de l'infraction (l'usurpation d'identité), on admet l'existence d'un concours parfait, et les deux dispositions s'appliquent. A titre d'exemple, si l'auteur prend sur un réseau social l'identité de B pour calomnier C, la nouvelle disposition punissant l'usurpation d'identité s'applique en sus de celle sanctionnant la calomnie. Il est ainsi possible de sanctionner le tort causé à B en incluant les conséquences négatives subies par celui-ci (atteinte à sa réputation, lancement d'une procédure, coûteux efforts pour faire laver sa réputation – avec plus ou moins de résultats). L'auteur d'une soustraction de données personnelles[238] à des fins d'usurpation d'identité sera également poursuivi en vertu des deux infractions (soustraction et usurpation). Si l'usurpation d'identité sert à commettre une escroquerie pour obtenir un avantage illicite, l'infraction d'escroquerie peut également englober celle d'usurpation (commise normalement en premier), de sorte que la sanction ordonnée couvre également cette dernière.

La sanction légale prévue doit être proportionnée à la valeur des biens juridiques qui sont protégés ou qui sont touchés par l'infraction, sans quoi la crédibilité et le pouvoir préventif du droit pénal se trouveraient réduits. Même si le bien juridique touché et les conséquences qui en découlent pour la victime ne sont pas forcément graves, il ne faut pas sous-estimer ni minimiser le danger que peut faire courir l'usurpation d'identité à l'ère numérique. Pour cette raison, la nouvelle infraction est considérée comme un délit, punie d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.

Les actes autorisés par la loi (qui sont par exemple commis dans le cadre d'une instruction policière ou d'une enquête pénale) demeurent licites en vertu de l'art. 14 CP.

Art. 352, al. 2

Il n'y a plus lieu de citer la loi en entier, le sigle étant introduit à l'art. 349*a* par la révision du CP figurant sous le ch. II P-LPD.

237 Pour un élément constitutif d'infraction identique dans le cadre d'un abus d'autorité, cf. Heimgartner Stefan, in: Niggli/Wiprächtiger (édit.), Basler Kommentar, Strafrecht II, 3e édition, Bâle 2013, ad art. 312 CP no 23.

238 Art. 179novies CP

Art. 355a, al. 1

La notion de «profil de la personnalité» est supprimée. Voir le commentaire au ch. 9.2.2.

Art. 365, al. 1, 1re phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire au ch. 9.2.2.

9.2.18 Loi fédérale du 22 mars 1974 sur le droit pénal administratif[239]

La loi sur le droit pénal administratif (DPA) s'applique lorsqu'une autorité administrative fédérale est chargée de poursuivre une infraction et de juger des infractions réprimées par la législation administrative fédérale (art. 1 et 2). En raison de la nouvelle teneur de l'art. 2, al. 3, P-LPD, il est nécessaire d'adopter des dispositions spéciales de protection des données dans la DPA, en reprenant la réglementation prévue dans le CPP avec les modifications apportées par le présent projet.

Art. 18a Collecte de données personnelles

Cette disposition règle la transparence de la collecte de données personnelles. Elle correspond à la réglementation prévue à l'art. 95 CPP.

Art. 18b Traitement de données personnelles

Voir par analogie le commentaire de l'art. 95*a* P-CPP (ch. 9.3.2).

Art. 18c Communication et utilisation de données personnelles dans le cadre d'une procédure pendante

Cette norme régit la communication et l'utilisation des données dans le cadre d'une procédure pendante. Elle correspond à la réglementation prévue à l'art. 96 CPP.

Art. 18d Droit aux renseignements dans le cadre d'une procédure pendante

Cette disposition règle le droit aux renseignements dans le cadre d'une procédure pendante. Elle correspond à la réglementation prévue à l'art. 97 CPP.

Art. 18e Exactitude des données personnelles

Cette disposition règle l'exactitude des données. Elle correspond à la réglementation prévue à l'art. 98 CPP. En ce qui concerne l'al. 2, il convient de se référer au commentaire de l'art. 98, al. 2, P-CPP (cf. ch. 9.3.2).

239 RS **313.0**

9.2.19 Procédure pénale militaire du 23 mars 1979[240]

La justice militaire est une autorité judiciaire indépendante (art. 1). Elle peut être assimilée à la notion de «tribunal» au sens de l'art. 2, al. 3, P-LPD. La procédure pénale militaire ne contient toutefois pas de dispositions propres de protection des données, contrairement au CPP. Le Conseil fédéral considère dès lors qu'il est opportun de compléter cette loi, en reprenant en grande partie la réglementation prévue dans le CPP avec les modifications apportées par le présent projet.

Art. 25a Collecte de données personnelles

Cette disposition règle la transparence de la collecte des données personnelles. Elle correspond à la réglementation prévue à l'art. 95 CPP.

Art. 25b Traitement de données personnelles

Voir par analogie le commentaire de l'art. 95*a* P-CPP (ch. 9.3.2).

Art. 25c Communication et utilisation de données personnelles dans le cadre d'une procédure pendante

Cette disposition règle la communication et l'utilisation de données personnelles dans le cadre d'une procédure pendante. Elle correspond à l'art. 96 CPP.

Art. 25d Droit aux renseignements dans le cadre d'une procédure pendante

Cette disposition règle le droit aux renseignements dans le cadre d'une procédure pendante. Elle correspond à l'art. 97 CPP.

Art. 25e Exactitude des données personnelles

Cette disposition règle l'exactitude des données. Elle correspond à l'art. 98 CPP. En ce qui concerne l'al. 2, il convient de se référer au commentaire de l'art. 98, al. 2, P-CPP.

9.2.20 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[241]

Art. 3, al. 2, 1re phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

240 RS **322.1**
241 RS **361**

Art. 5, titre et al. 2

Le Conseil fédéral considère que l'al. 2 peut être abrogé. La sous-traitance du traitement de données, y compris à des fins de contrôle et de maintenance informatique, est réglée à l'art. 8 P-LPD. Le titre de cette disposition doit être adapté en conséquence.

Art. 7, al. 1

Le renvoi au P-LPD est adapté.

9.2.21 Loi du 4 octobre 1991 sur les EPF[242]

Art. 36a, al. 1, 1re phrase, 36b, al. 1 et 5, 2e phrase, et 36c

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2. Le renvoi au P-LPD est par ailleurs adapté à l'art. 36c, al. 2.

9.2.22 Loi du 17 juin 2011 sur l'encouragement du sport[243]

Art. 21, al. 3, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 25, al. 1, phrase introductive, et 4

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2. L'al. 4 règle la communication des données personnelles aux autorités compétentes d'un Etat tiers en prévoyant un renvoi aux art. 13 et 14 P-LPD.

9.2.23 Loi fédérale du 19 juin 2015 sur les systèmes d'information de la Confédération dans le domaine du sport[244]

Art. 1, al. 1, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

242 RS **414.110**
243 RS **415.0**
244 RS **415.1**

Art. 4

Cette disposition règle le traitement de données aux fins de travaux sur les systèmes d'information. Elle peut être abrogée. En effet, la sous-traitance du traitement de données, y compris à des fins de contrôle et de maintenance informatique, est régie à l'art. 8 P-LPD.

Art. 9, phrase introductive, 14, phrase introductive, 18, phrase introductive, 22, phrase introductive, 26, phrase introductive et 32, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.24 Loi du 9 octobre 1992 sur la statistique fédérale[245]

En raison de l'abrogation de la protection des données personnelles des personnes morales, certaines dispositions de la loi sur la statistique fédérale doivent être modifiées (cf. ch. 9.1.11). Dans le domaine des statistiques, le Conseil fédéral est de l'avis que le même niveau de protection doit être garanti pour les personnes physiques et morales. Certains termes sont également adaptés à la nouvelle terminologie du P-LPD.

Art. 5, al. 2, let. a, et 4, let. a

Le terme «données personnelles» est remplacé par ceux de «données personnelles et données concernant des personnes physiques ou morales».

Art. 7, al. 2

La notion de «fichier» est remplacée par celle de «banque de données» (cf. commentaire sous ch. 9.2.2). Le renvoi à l'art. 22 LPD doit être adapté à la nouvelle numérotation du P-LPD (art. 35).

Art. 10, al. 4 et 5

A l'al. 4, les termes «des données provenant de leurs fichiers» sont remplacés par «des données personnelles provenant de leurs banques de données».

A l'al. 5, le renvoi au P-LPD est adapté.

Art. 12, al. 2

La notion de «fichier» est remplacée par celle de «banque de données».

245 RS **431.01**

Art. 14, al. 1

La notion de «personne concernée» est remplacée par les termes «la personne physique ou morale concernée».

Art. 14a, al. 1, 2e phrase

La notion de «données personnelles sensibles» est remplacée par les termes «données personnelles sensibles et données sensibles concernant des personnes morales». La notion de «profils de la personnalité» est remplacée par les termes «les caractéristiques essentielles d'une personne physique ou morale».

Art. 15, al. 1

La notion de «données personnelles» est remplacée par les termes «données personnelles et données concernant des personnes morales». Le principe de sécurité doit valoir pour ces deux catégories de personnes.

Art. 16, al. 1

En raison de l'abrogation de la protection des données concernant des personnes morales, il y a lieu de préciser que seuls les traitements de données personnelles concernant des personnes physiques sont régis par la future LPD.

Art. 19, al. 2, phrase introductive

Le terme «données personnelles» est remplacé par «données personnelles et données concernant des personnes morales».

9.2.25 Loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises[246]

Art. 3, al. 1, let. d, et 5, al. 1, let. b

La notion de «fichier» est remplacée par celle de «banque de données». Voir le commentaire sous ch. 9.2.2.

9.2.26 Loi du 18 décembre 1992 sur la Bibliothèque nationale[247]

Art. 2, al. 2, et 7

Ne concerne que le texte allemand. Il s'agit de remplacer la notion de «*Datensammlung*» par celle de «*Datenbank*» aux art. 2, al. 2, et 7.

246 RS **431.03**
247 RS **432.21**

9.2.27 Loi du 16 mars 2012 sur les espèces protégées[248]

Art. 23, al. 2, 1re phrase

Le droit en vigueur prescrit d'une part que les données peuvent être communiquées en ligne si la législation étrangère assure un niveau de protection adéquat de la personnalité des personnes concernées et que d'autre part le Conseil fédéral désigne les pays et les organisations supranationales et internationales qui présentent cette garantie. Pour garantir une réglementation uniforme en droit fédéral, il convient de faire un renvoi à l'art. 13 P-LPD.

9.2.28 Loi fédérale du 16 décembre 2005 sur la protection des animaux[249]

Art. 20c, al. 1, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.29 Loi du 3 février 1995 sur l'armée[250]

Art. 31, al. 2, 2e phrase

L'art. 31, al. 1, prévoit que des services sont à la disposition des militaires pour leur prodiguer conseils et assistance dans les domaines médical, spirituel, psychologique ou social en relation avec le service militaire. Compte tenu de la nature de ces tâches, il y a lieu de supprimer la notion de «profil de la personnalité» à l'al. 2.

Art. 99, al. 2, 1re phrase, et 3, let. d

En raison de la nature des tâches du service de renseignement de l'armée, il y a lieu de remplacer la notion de «profil de la personnalité» par celle de «données personnelles qui permettent d'évaluer la menace qu'une personne représente» à l'al. 2, 1re phrase. Cette modification correspond aux exigences de base légale de l'art. 30, al. 2, let. c, P-LPD.

A l'al. 3, let. d, la notion de «fichier» est remplacée par celle de «activité de traitement». Voir le commentaire du ch. 9.2.2.

248 RS **453**
249 RS **455**
250 RS **510.10**

Art. 31, al. 2, 2e phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 146

Il y a lieu de remplacer la notion de «profil de la personnalité» par celle de «données personnelles qui permettent d'évaluer la menace qu'une personne représente».

9.2.30 Loi du 5 octobre 2007 sur la géoinformation[251]

Art. 11 Protection des données

L'*al. 1* correspond à l'art. 11 de la loi sur la géoinformation en vigueur. Il établit que les dispositions de la nouvelle LPD s'appliquent à toutes les géodonnées de base de droit fédéral constituant des données personnelles. Avec ce renvoi, et comme le mentionne le message relatif à la loi fédérale du 6 septembre 2006 sur la géoinformation[252]: «une règle uniforme vaut pour toutes les géodonnées de base de droit fédéral en matière de protection des données, à savoir celle fixée par la Confédération, et cela quel que soit l'auteur du traitement des géodonnées à caractère personnel: administration fédérale, cantonale, communale ou acteur du secteur privé agissant dans le cadre d'un mandat conféré par les autorités. Dans le cas de géodonnées de base de droit fédéral constituant des données personnelles et dont la maîtrise est attribuée aux cantons ou aux communes, la surveillance de la protection des données reste du ressort des autorités de surveillance de la protection des données cantonales ou communales en dépit de l'applicabilité de la LPD».

Dans la mesure où des géodonnées de base de droit fédéral constituent des données personnelles, elles doivent, conformément à l'art. 11 P-LPD, figurer sur le registre des activités de traitement. Etant donné que la plupart des géodonnées de droit fédéral permettent, à partir de la géométrie du terrain, du numéro de l'immeuble et des données publiques du registre foncier, d'établir un lien indirect avec le propriétaire, il faudrait que la Confédération et les cantons intègrent dans les registres des activités de traitement environ 50 des quelque 190 jeux de géodonnées de base. Cela aurait peu de sens du point de vue de la protection des données, dans la mesure où toutes les géodonnées de base de droit fédéral figurent déjà en annexe de l'ordonnance du 21 mai 2008 sur la géoinformation[253] et où la plupart d'entre elles sont accessibles au public en vertu d'une loi spéciale. C'est la raison pour laquelle l'*al. 2* autorise le Conseil fédéral à exclure l'inscription des géodonnées de base sur le registre des activités de traitement dès lors qu'elles ne portent pas atteinte aux droits fondamentaux.

L'*al. 3* dispose que le Conseil fédéral peut fixer, concernant les géodonnées de base de droit fédéral, des niveaux d'autorisation d'accès qui tiennent compte de tous les

251 RS **510.62**
252 FF **2006** 7407, 7442
253 RS **510.620**

aspects de la protection des données, des obligations spéciales de garder le secret et du principe de transparence. Cette règle, applicable par voie d'ordonnance depuis l'entrée en vigueur de la législation sur la géoinformation en 2008, a fait ses preuves et doit être inscrite dans la loi. Ces niveaux d'autorisation d'accès concernent l'accès de tiers et d'autorités aux géodonnées. Des exceptions au droit d'accès de la personne concernée sur ses propres données ne sont admises qu'aux conditions de l'art. 24 P-LPD.

9.2.31 Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[254]

Art. 1, al. 1, phrase introductive, et al. 3

La notion de «profils de la personnalité» peut être remplacée par celle de «données personnelles». En effet, le catalogue des données personnelles qui peuvent être traitées est défini dans les dispositions légales applicables au système d'information concerné.

Le renvoi au P-LPD est adapté à l'al. 3.

Art. 10, let. c

Il s'agit d'adapter la terminologie à celle de l'art. 4, let. c, ch. 2, P-LPD.

Art.11, al. 2

L'art. 11 prévoit une restriction du traitement lorsqu'il y a une combinaison de certaines données. Le terme «profil de la personnalité» est décrit d'une manière différente, comme des données dont le rapprochement permet d'apprécier les caractéristiques essentielles de la personnalité. L'al. 2 fixe un délai de conservation maximal pour ces types de données.

9.2.32 Loi fédérale du 13 décembre 1996 sur le matériel de guerre[255]

Art. 30, al. 2, 2e phrase

Dans le cadre de l'application de la loi sur le matériel de guerre, l'Office central pour la répression du trafic illicite du matériel de guerre participe à la prévention des infractions et a pour tâche de dénoncer les infractions aux dispositions de cette loi aux autorités compétentes en matière de poursuite pénale. A cette fin, l'art. 30, al. 2, 2e phrase, prévoit que l'office central a le droit de traiter des données personnelles, y compris des données sensibles et des profils de la personnalité, dans la mesure et

254 RS **510.91**
255 RS **514.51**

aussi longtemps que l'exécution de ses tâches l'exige. Au vu de la nature des tâches de l'office central, la notion de «profil de la personnalité» doit être remplacée par celle de «données personnelles qui permettent d'évaluer le risque qu'une personne commette une infraction».

9.2.33 Loi fédérale du 20 juin 1997 sur les armes[256]

Art. 32e, al. 1 et 2

Voir le commentaire de l'art. 111*d*, al. 1 et 2, P-LEtr (ch. 9.2.3).

Art. 32g, 2e phrase

Voir le commentaire de l'art. 111*f*, 2e phrase, P-LEtr (ch. 9.2.3).

9.2.34 Loi fédérale du 4 octobre 2002 sur la protection de la population et sur la protection civile[257]

Art. 72, al. 1, 2e phrase introductive et let. a et b, et 1bis

Le droit en vigueur prévoit que l'autorité fédérale compétente est habilitée à établir des profils de la personnalité pour déterminer le potentiel de cadre des personnes astreintes et des participants aux cours. Il y a lieu dès lors de remplacer, à l'al. 1, la notion de «profils de la personnalité» par les termes suivants «des données personnelles permettant d'évaluer l'affectation d'une personne astreinte à une fonction de base ou pour déterminer son potentiel de cadre». A l'al. 1bis, la notion de «profil de la personnalité» est remplacée par les termes suivants «données personnelles permettant de déterminer le potentiel de cadre ou de spécialiste».

9.2.35 Loi du 7 octobre 2005 sur les finances[258]

Art. 60c, al. 1, phrase introductive, et 3

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

256 RS **514.54**
257 RS **520.1**
258 RS **611.0**

9.2.36 Loi du 28 juin 1967 sur le Contrôle des finances[259]

Art. 10, al. 3

La modification ne concerne que le texte allemand. Il s'agit de supprimer la notion de «*Datensammlung*» dans la première phrase et de remplacer ce terme dans la dernière phrase par celui de «*System*».

9.2.37 Loi du 18 mars 2005 sur les douanes[260]

Art. 38, al. 2

La décision de taxation visée à l'art. 1 peut être prise sous la forme d'une décision individuelle automatisée au sens de l'art. 19 P-LPD. Conformément à l'art. 19, al. 4, P-LPD, l'autorité doit signaler cette décision comme telle afin que la personne concernée puisse se rendre compte qu'elle n'émane pas d'une personne physique.

Art. 103, al. 1, phrase introductive, et 2

L'Administration fédérale des douanes (AFD) peut aussi établir l'identité d'une personne en relevant des données génétiques. Cette disposition, qui figurait jusqu'ici à l'art. 226, al. 3, let. b, ch. 1, de l'ordonnance du 1er novembre 2006 sur les douanes[261], est transférée dans la loi.

Art. 110, al. 1 et 2

A l'al. 1, la notion de «profil de la personnalité» est supprimée. Les finalités prévues à l'al. 2 selon le droit en vigueur sont dorénavant réglées à l'al. 1.

La première phrase du nouvel al. 2 se limite à prévoir que l'AFD peut gérer des systèmes d'information à cet effet. La seconde phrase de l'al. 2 est nouvelle. Elle autorise l'AFD à faire du profilage pour les tâches énumérées à l'al. 1, à l'exception de celle prévue à l'al. 1, let. d. L'AFD procède en effet au traitement et à l'analyse automatisés de données personnelles afin d'établir des profils de risque qui lui permettent de mieux focaliser ses contrôles. Pour ce faire, elle a besoin d'une base légale au sens formel.

Art. 110a, al. 3, let. b

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

259 RS **614.0**
260 RS **631.0**
261 RS **631.01**

Art. 112, al. 2, phrase introductive, 4, let. b et 6, 2e phrase

La notion de «profil de la personnalité» à la phrase introductive de l'al. 2 est supprimée. Voir le commentaire du ch. 9.2.2.

L'al. 2 doit en outre prévoir une base légale pour la communication de données personnelles issues d'un profilage (cf. le commentaire de l'art. 32 P-LPD au ch. 9.1.7).

L'al. 4, let. b, peut être abrogé au motif qu'il n'est plus applicable.

Le renvoi au P-LPD de l'al. 6, 2e phrase est adapté.

Art. 113 et 114, al. 2

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. ch. 9.2.2.

Les deux dispositions doivent en outre prévoir une base légale pour la communication de données personnelles issues d'un profilage (cf. le commentaire de l'art. 32 P-LPD au ch. 9.1.7).

9.2.38 Loi du 12 juin 2009 sur la TVA[262]

Art. 76, al. 1, 2e phrase

Le droit en vigueur prévoit que l'Administration fédérale des contributions gère les fichiers ainsi que les moyens de traitement et de conservation des données nécessaires. Cette disposition est superflue. Elle peut être abrogée.

9.2.39 Loi fédérale du 21 mars 1969 sur l'imposition du tabac[263]

Art. 18, al. 4

La fixation du montant de l'impôt peut revêtir la forme d'une décision individuelle automatisée au sens de l'art. 19 P-LPD. Conformément à l'art. 19, al. 4, P-LPD, l'autorité doit signaler cette décision comme telle afin que la personne concernée puisse se rendre compte qu'elle n'émane pas d'une personne physique.

262 RS **641.20**
263 RS **641.31**

9.2.40 Loi fédérale du 6 octobre 2006 sur l'imposition de la bière[264]

Art. 17, al. 3, 2e phrase

Voir le commentaire du projet d'art. 18, al. 4 de la loi sur l'imposition du tabac (ch. 9.2.39).

9.2.41 Loi fédérale du 21 juin 1996 sur l'imposition des huiles minérales[265]

Art. 21, al. 2bis

Voir le commentaire du projet d'art. 18, al. 4 de la loi sur l'imposition du tabac (ch. 9.2.39).

9.2.42 Loi du 19 décembre 1997 relative à une redevance sur le trafic des poids lourds[266]

Art. 11, al. 4

Voir le commentaire du projet d'art. 18, al. 4 de la loi sur l'imposition du tabac (ch. 9.2.39).

9.2.43 Loi du 21 mars 2003 sur l'énergie nucléaire[267]

Art. 24, al. 2

Le droit en vigueur prévoit que le contrôle de fiabilité des personnes exerçant des fonctions en matière de sécurité peut donner lieu au traitement de données sensibles sur la santé et le psychisme de ces personnes, ainsi que de données sur leur mode de vie importantes pour la sécurité, et qu'un fichier à ce sujet peut être constitué. La seconde phrase peut être supprimée car elle est superflue.

264 RS **641.411**
265 RS **641.61**
266 RS **641.81**
267 RS **732.1**

9.2.44 Loi fédérale du 24 juin 1902 sur les installations électriques[268]

Art. 25a, al. 2

La partie de phrase «Elles peuvent conserver ces données dans un fichier électronique» peut être supprimée car elle est inutile.

9.2.45 Loi fédérale du 19 décembre 1958 sur la circulation routière[269]

Art. 76b, al. 3, 2e phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.46 Loi fédérale du 20 décembre 1957 sur les chemins de fer[270]

Art. 16a Traitement de données par des concessionnaires

Les renvois de l'*al. 1* aux articles de la future LPD doivent être adaptés. L'al. 1 de la version allemande subit diverses modifications afin d'aligner ce texte sur les versions française et italienne.

La notion de «profil de la personnalité» est supprimée à l'*al. 2*. Voir le commentaire du ch. 9.2.2.

L'*al. 3* prescrit que la surveillance des traitements de données personnelles effectués par les entreprises ferroviaires concessionnaires est régie par l'art. 27 LPD. Cet alinéa peut être supprimé au motif que le P-LPD ne fait plus de différence selon que le préposé exerce une surveillance sur une personne privée ou sur un organe fédéral.

9.2.47 Loi fédérale du 20 mars 2009 sur le transport des voyageurs[271]

Art. 54 Traitements de données par les concessionnaires

Voir le commentaire du projet d'art. 16*a* de la loi sur les chemins de fer (ch. 9.2.46).

268 RS **734.0**
269 RS **741.01**
270 RS **742.101**
271 RS **745.1**

9.2.48 Loi du 4 octobre 1963 sur les installations de transport par conduites[272]

Art. 47a, al. 2

Voir le commentaire du projet d'art. 25*a*, al. 2, de la loi fédérale sur les installations électriques (ch. 9.2.44).

9.2.49 Loi fédérale du 21 décembre 1948 sur l'aviation[273]

Art. 107a, al. 2, phrase introductive, 4 et 5

La notion de «profil de la personnalité» dans la phrase introductive de l'al. 2 est supprimée. Cette suppression n'a pas de conséquence sur la base légale prévue à la let. a, ch. 1 à 3.

La modification apportée à l'al. 4 ne concerne que le texte allemand. Il s'agit en effet de remplacer la notion de «*Datensammlung*» par celle de «*Datenbeschaffung*».

A l'al. 5, la notion de «profils de la personnalité» est supprimée. La communication des données personnelles à des autorités étrangères est possible pour autant que les conditions de l'art. 13 P-LPD soient respectées.

Il convient de signaler la modification du 16 juin 2017 de la loi sur l'aviation[274]. Lors de l'élaboration des normes de coordination (cf. ch. 13.7), il s'agira le cas échéant de supprimer à l'art. 21*c*, al. 1, let. b, la notion de «profil de la personnalité».

9.2.50 Loi du 17 décembre 2010 sur la poste[275]

Art. 26, al. 1, 2, phase introductive, 3, 2e phrase, et 28

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.51 Loi du 30 avril 1997 sur les télécommunications[276]

Art. 13a, al. 1, 1re phrase, et 13b, al. 1, 2e phrase, 2, phrase introductive, et 4, 1re phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

272 RS **746.1**
273 RS **748.0**
274 FF **2017** 3993
275 RS **783.0**
276 RS **784.10**

9.2.52 Loi fédérale du 24 mars 2006 sur la radio et la télévision[277]

Art. 69f, al. 1, 2e phrase, et 88, al. 2

Ces dispositions prescrivent que le traitement de données personnelles et sa surveillance sont régis par les dispositions de la LPD applicables aux organes fédéraux. Le terme «sa surveillance» doit être abrogé au motif que le P-LPD ne fait plus de différence selon que le préposé exerce une surveillance sur une personne privée ou sur un organe fédéral.

9.2.53 Loi du 30 septembre 2011 relative à la recherche sur l'être humain[278]

Art. 42, al. 2

Il y a lieu de renvoyer aux art. 13 et 14 P-LPD et non plus à l'art. 6 LPD.

9.2.54 Loi du 3 octobre 1951 sur les stupéfiants[279]

Art. 3f, al. 1

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 18c, 2e phrase

Voir le commentaire de l'art. 111*f*, 2e phrase, P-LEtr (ch. 9.2.3).

9.2.55 Loi du 28 septembre 2012 sur les épidémies[280]

Art. 60, al. 9, 1re phrase

Les renvois au P-LPD sont adaptés.

277 RS **784.40**
278 RS **810.30**
279 RS **812.121**
280 RS **818.101**

Art. 62, al. 1 et 3, phrase introductive et let. a et d

L'art. 62 règle la communication des données personnelles à des autorités étrangères. Les modifications s'alignent sur la nouvelle réglementation prévue aux art. 13 et 14 P-LPD.

9.2.56 Loi du 17 juin 2005 sur le travail au noir[281]

Art. 17 titre et al. 1, phrase introductive, 2 et 4

En raison de l'abrogation de la protection des données concernant des personnes morales, il est nécessaire de créer deux bases légales distinctes (voir aussi ch. 9.1.11). L'art. 17 règle dorénavant uniquement le traitement de données personnelles par les autorités cantonales compétentes.

A l'al. 4, le renvoi au P-LPD est adapté.

Art. 17a

L'art. 17*a* habilite les autorités cantonales compétentes à traiter des données concernant des personnes morales.

9.2.57 Loi fédérale du 6 octobre 1989 sur le service de l'emploi et la location de services[282]

Art. 33a, al. 1, phrase introductive, et 1bis, et 35, al. 2, 3bis et 5, let. d

Comme il ressort du message du Conseil fédéral du 24 novembre 1999 concernant l'adaptation et l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales[283], les organes qui participent à l'exécution de la législation sur les assurances sociales, qui englobe, au sens large, également la loi fédérale sur le service de l'emploi et la location de services (LSE), sont appelés à traiter de manière constante une foule de données personnelles, dès l'assujettissement à l'assurance, au moment du calcul et du prélèvement des cotisations ou des primes, ou encore au moment de la détermination et de l'allocation des prestations d'assurance. Les données personnelles traitées sont de nature fort diverse. Il peut s'agir de données sur l'identité d'une personne, de données sensibles concernant la santé ou encore d'indications relevant de la sphère privée telles que l'âge, les revenus, le parcours professionnel, l'histoire familiale, etc. Suivant la manière dont elles doivent éventuellement être assemblées, des données personnelles peuvent fournir un aperçu de la personnalité d'un individu et former ainsi des «profils de la personnalité» au sens de l'art. 3, let. d, LPD.

281 RS **822.41**
282 RS **823.11**
283 FF **2000** 219

Le projet de loi abroge la notion de «profil de la personnalité» et donc la base légale y relative prévue à l'art. 33*a* LSE. Le Conseil fédéral considère toutefois que les traitements permettant de donner un aperçu de la personnalité d'un individu, tels qu'ils sont décrits au paragraphe précédent, ne sauraient être poursuivis sans une base légale au sens formel (art. 30, al. 2, let. c, P-LPD). Dans le domaine des assurances sociales, de tels traitements sont en effet susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée. Le Conseil fédéral propose par conséquent de compléter l'art. 33*a* par un nouvel al. 3 qui habilite les organes compétents à traiter des données personnelles permettant d'évaluer la situation personnelle et économique des bénéficiaires de prestations de conseil au sens de l'al. 1.

Art. 35b Registre des entreprises de placement et de location de services autorisés

La notion de «fichier» est remplacée par celle de «registre». Voir le commentaire du ch. 9.2.2.

9.2.58 Loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[284]

Art. 49a, al. 1, phrase introductive, et 2

Le projet de loi abroge la notion de «profil de la personnalité» et donc la base légale y relative prévue à l'art. 49*a*. Comme pour la LSE (cf. ch. 9.2.57), le Conseil fédéral estime toutefois qu'il est nécessaire de créer une base légale au sens formel pour certains traitements de données qui permettent de fournir un aperçu de la personnalité d'un individu (art. 30, al. 2, let. c, P-LPD). De tels traitements sont en effet susceptibles de porter gravement atteinte aux droits fondamentaux de la personne concernée, surtout s'ils portent également sur des données sensibles d'ordre médical. Le Conseil fédéral propose par conséquent de compléter l'art. 49*a* par un nouvel al. 2 qui habilite les organes compétents à traiter des données personnelles qui permettent d'évaluer notamment la santé, la gravité de l'affection physique ou psychique, les besoins et la situation économique de la personne assurée pour les tâches mentionnées à l'al. 1.

9.2.59 Loi fédérale du 25 juin 1982 sur la prévoyance professionnelle vieillesse, survivants et invalidité[285]

Art. 85a, al. 1, phrase introductive, et 2

Voir le commentaire de l'art. 49*a* P-LAVS (ch. 9.2.58).

284 RS **831.10**
285 RS **831.40**

9.2.60 Loi fédérale du 18 mars 1994 sur l'assurance-maladie[286]

Art. 84, al. 1, phrase introductive, et 2

Voir le commentaire de l'art. 49*a* P-LAVS (ch. 9.2.58).

Concernant le nouvel art. 84, al. 2, de la loi fédérale sur l'assurance-maladie (LAMal), on peut également renvoyer pour l'essentiel à l'explication sur l'art. 49*a*, al. 2, P-LAVS (cf. ch. 9.2.58). En comparaison des autres assurances sociales, cette disposition trouve à s'appliquer dans l'assurance-maladie sociale, principalement pour les indemnités journalières. Dans le domaine de l'assurance obligatoire des soins, et des tâches des assurances qui y sont liées, on doit compter sur une application restrictive de cette disposition dans le cadre des tâches légales, par exemple lorsque des informations complémentaires sont nécessaires dans un cas concret, comme pour le remboursement de certains médicaments. Il faut retenir que le traitement des catégories de données citées à l'al. 2 n'est en aucun cas admis pour un but sortant de la mise en œuvre de l'assurance obligatoire des soins et des indemnités journalières.

9.2.61 Loi fédérale du 20 mars 1981 sur l'assurance-accidents[287]

Art. 96, al. 1, phrase introductive, et 2

Seule modification apportée à l'al. 1 de la loi fédérale sur l'assurance-accidents (LAA): la suppression de la notion de profils de la personnalité dans la phrase introductive.

L'al. 2 est nouveau. Il dispose que les organes visés à l'al. 1 sont habilités, afin d'exécuter leurs tâches prévues à ce même al. 1, à procéder au profilage et à des décisions individuelles automatisées.

L'assurance-accidents obligatoire repose sur le principe des prestations en nature. L'assureur doit fournir les prestations de soins en nature, à ses frais, ce qui fait de lui le débiteur du fournisseur des prestations[288]. Il fournit donc au patient une gamme de soins complète et appropriée plutôt que de rembourser les frais contre facture, comme c'est le cas dans l'assurance-maladie (principe du remboursement des frais).

Le principe des prestations en nature permet notamment à l'assureur de co-déterminer l'ampleur, la nature et la durée des prestations, afin de prendre les mesures qu'exige le traitement approprié de l'assuré (art. 48, al. 1, LAA). Le traitement approprié de l'assuré peut, dans certaines circonstances, éviter le versement futur d'une rente. Pour pouvoir déterminer ce traitement, l'assureur doit avoir accès aux

286 RS **832.10**
287 RS **832.20**
288 Maurer Alfred, Schweizerisches Unfallversicherungsrecht, 2e éd., Berne 1989, pp. 523 ss.

données médicales nécessaires. Le profilage lui permettra par exemple d'identifier des cas complexes à un stade précoce et de les confier à un collaborateur spécialisé.

Dans l'ensemble, le nouvel al. 2 ne confère aucune compétence nouvelle aux assureurs; il leur permet simplement de continuer à exercer leurs compétences actuelles.

9.2.62 Loi fédérale du 19 juin 1992 sur l'assurance militaire[289]

Art. 94a, al. 1, phrase introductive, et 2

Voir le commentaire de l'art. 96 P-LAA (ch. 9.2.58).

9.2.63 Loi fédérale du 25 juin 1982 sur l'assurance-chômage[290]

Art. 96b, al. 1, phrase introductive, et 2, et 96c, al. 2, phrase introductive, et 2bis

Voir le commentaire de l'art. 49*a* P-LAVS (ch. 9.2.58).

9.2.64 Loi du 1er juillet 1966 sur les épizooties[291]

Art. 54a, al. 3

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

9.2.65 Loi du 20 juin 1986 sur la chasse[292]

Art. 22, al. 3, 1re et 2e phrases

La notion de «fichier électronique» est supprimée, tandis que le terme d'«inscriptions électroniques» est remplacé par celui de «données personnelles».

289 RS **833.1**
290 RS **837.0**
291 RS **916.40**
292 RS **922.0**

9.2.66 Loi du 3 octobre 2003 sur la Banque nationale[293]

Art. 14, al. 3

Conformément à l'art. 14, al. 1, de la loi sur la Banque nationale (LBN), cette dernière relève les données statistiques nécessaires pour l'exercice de ses tâches légales et l'observation de l'évolution des marchés financiers. Pour limiter la charge de l'obligation de déclarer et éviter autant que possible les recoupements avec la collecte de données d'autres services statistiques ou unités administratives de la Confédération, elle collabore avec les services compétents de la Confédération, en particulier l'Office fédéral de la statistique (OFS) et la FINMA, mais aussi avec les autorités compétentes d'autres pays et avec des organisations internationales (art. 14, al. 2, LBN).

La pratique a démontré que les règles actuelles n'étaient pas suffisantes. Ainsi, les règles sur l'obligation du secret et sur le blocage interdisent dans certains cas une transmission de données non agrégées à la Banque nationale. De même, l'art. 74 de la loi du 12 juin 2009 sur la TVA[294] interdit une transmission des données sur la TVA de l'Administration fédérale des contributions (AFC) à la Banque nationale. L'AFC peut certes mettre ces données à la disposition de l'OFS sous une forme non anonymisée (art. 10, al. 4 et 5, de la loi du 9 octobre 1992 sur la statistique fédérale [LSF][295] et art. 136, al. 2, de l'ordonnance du 27 novembre 2009 sur la taxe sur la valeur ajoutée[296]). Une transmission de l'AFC à la Banque nationale est en revanche exclue, parce que la LBN ne contient pas de disposition analogue à l'art. 10, al. 4 et 5, LSF. Il en résulte que les données pour la Banque nationale, déjà existantes auprès de l'AFC, doivent être à nouveau récoltées. Cela conduit à une double charge de travail.

L'art. 14 doit ainsi être complété d'un nouvel al. 3. Par analogie à la règle de la LSF, il est prévu que l'AFC fournira à la Banque nationale, pour que celle-ci accomplisse ses tâches statistiques, les bases et les résultats de ses travaux statistiques concernant la TVA et, au besoin, les données provenant de ses dossiers et de ses relevés. Avec cette règle, il est assuré que la Banque nationale, dans le domaine de la TVA, ne doive pas collecter elle-même une nouvelle fois des données déjà existantes auprès de l'AFC.

Pour s'assurer que des tiers n'accèdent pas à des données auxquelles ils ne pourraient avoir accès auprès de la Banque nationale, il est prévu expressément que celle-ci ne peut pas transmettre les données reçues de l'AFC en vertu de l'al. 3 à des tiers. Cette limite vaut aussi, malgré l'art. 35 P-LPD, pour la communication de données à des tiers pour des buts non-individuels, en particulier pour la recherche, la planification et la statistique. La Banque nationale est également limitée dans le partage de ces données avec la FINMA, malgré l'art. 16, al. 4, avec l'OFS, malgré l'art. 16, al. 4bis, ou avec des banques centrales étrangères ou des organisations ou organes internationaux, malgré les art. 50*a* et 50*b* LBN. Une transmission des données sous forme agrégée est en revanche autorisée dans le cadre de l'art. 16, al. 3, LBN.

293 RS **951.11**
294 RS **641.20**
295 RS **431.01**
296 RS **641.201**

Art. 16, al. 4bis et 5

L'art. 16 règle la confidentialité des données traitées par la Banque nationale à des fins statistiques.

La Banque nationale doit garder le secret sur les données qu'elle collecte et cela aussi à l'encontre de chaque autorité ou organisation internationale avec lesquelles elle a un devoir de collaboration statistique. En conséquence, elle ne peut, selon le droit en vigueur, partager les données confidentielles qu'avec les autorités suisses compétentes en matière de surveillance des marchés financiers (art. 16, al. 4, LBN). Pour toutes les autres autorités nationales ou étrangères, en particulier l'OFS, la Banque nationale ne peut formellement leur transmettre des données collectées que sous forme agrégée (art. 16, al. 3, qui renvoie à l'art. 14, al. 2, LBN). La seule exception, hors la FINMA, est constituée par les banques pour la compensation des paiements internationaux et certaines organisations et organes internationaux à qui la banque nationale peut transmettre, depuis peu et à des conditions strictes, des informations qui ne sont pas ouvertement accessibles (y compris les données statistiques; art. 50*a* et 50*b* LBN).

Pour l'analyse du développement des marchés financiers, la vue d'ensemble des transactions financières, l'établissement de la balance des paiements ou pour les statistiques sur les avoirs à l'étranger, la Banque nationale collecte des données auprès de personnes physiques et morales sur leurs activités commerciales (art. 15, al. 2, LBN). Rien que dans le domaine de la balance des paiements, il y a de nombreux recoupements entre les besoins en données de la Banque nationale et ceux de l'OFS. Le manque d'un principe légal clair pour la communication de données de la Banque nationale à l'OFS conduit ainsi à ce que ces deux autorités doivent fournir d'importants efforts pour leur collecte de données et pour s'assurer de la qualité de celles-ci. Des synergies entre les collectes ne peuvent être trouvées. Cela conduit non seulement la Banque nationale et l'OFS, mais aussi en particulier ceux qui sont tenus de fournir les renseignements, à une charge supplémentaire de travail qui pourrait être évitée par la possibilité d'échanger des données. S'ajoute à cet argument que la Banque nationale, comme l'OFS et les autres services statistiques, doivent limiter leur collecte de données au strict minimum et maintenir un niveau de charge administrative le plus faible possible (art. 4, al. 1, de l'ordonnance du 18 mars 2004 sur la banque nationale [OBN][297]). En particulier, la Banque nationale doit éviter une collecte de données si elle peut «se procurer, par un autre moyen, des données de qualité équivalente» (art. 4, al. 3, OBN).

Pour ces raisons, la Banque nationale doit obtenir la compétence de transmettre des données non agrégées à l'OFS. Comme il s'agit d'une exception au principe de l'al. 3, qui impose à la Banque nationale de ne transmettre des données à d'autres autorités nationales ou étrangères et aux organisations internationales que sous forme agrégée, la règle est appliquée lorsque le transfert de données a lieu dans un but statistique et que l'OFS a besoin de ces données pour l'exécution de ses tâches. Dans le nouvel alinéa il est clairement établi que l'OFS ne peut transmettre ces données à des tiers. Cette interdiction vaut aussi, malgré la règle générale de l'art. 35 P-LPD, pour les transmissions dans un but non-individuel. Il est aussi expressément

297 RS **951.131**

exclu de transmettre ces données à d'autres services ou autorités statistiques internes ou internationaux. Avec cette interdiction de transmission, on empêche que des tiers puissent obtenir de l'OFS des données auxquelles ils n'auraient pas accès.

Contrairement à la Banque nationale, l'OFS est autorisé aujourd'hui déjà, en vertu de l'art. 19, al. 2, LSF, à partager avec la Banque nationale des données personnelles non agrégées à des fins statistiques et à certaines conditions. Cette règle vaut pour les données du registre des entreprises et des établissements (REE) mais de manière limitée. Ainsi l'OFS, en vertu de l'art. 10, al. 5, LSF, ne peut pas transférer les données du REE concernant la TVA. Avec le nouvel art. 14, al. 3, LBN, la base légale pour un transfert direct des données sur la TVA de l'AFC à la Banque nationale à des fins statistiques est créée.

La modification de l'art. 16, al. 5, découle de la modification du champ d'application de la LPD. Vu que cette disposition vise toute sorte de données, y compris des données concernant des personnes morales, il est nécessaire de préciser à l'al. 5 que seules les données concernant des personnes physiques sont régies par la future LPD.

Art. 49a Traitements de données personnelles et de données concernant des personnes morales

Dans le cadre de sa mission officielle, la Banque nationale traite une multitude de données concernant des personnes morales et, dans une moindre mesure, physiques. Ces renseignements sur les acteurs des marchés financiers et les entreprises lui sont indispensables pour accomplir ses tâches légales. Dans les domaines de la statistique (art. 14 à 16 LBN) et de la stabilité financière (art. 16*a* LBN), la Banque nationale jouit d'une base légale explicite pour le traitement de données. Par mesure de sécurité juridique, l'art. 49*a* précise qu'elle peut, afin d'accomplir ses tâches légales, traiter des données personnelles, y compris des données sensibles, ainsi que des données concernant des personnes morales.

9.2.67 Loi fédérale du 10 octobre 1997 sur le blanchiment d'argent[298]

Art. 29, al. 2, 2e phrase

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Art. 33 Principes

Le renvoi au P-LPD est adapté.

298 RS **955.0**

Art. 34, titre et al. 1 à 3

La notion de «fichier» est remplacée par celle de «dossiers et banque de données» dans le titre et dans les al. 1 et 3.

Le renvoi au P-LPD est adapté à l'al. 3.

9.2.68 Loi du 22 juin 2007 sur la surveillance des marchés financiers[299]

Art. 23 Traitement de données

La présente révision abroge la notion de «profil de la personnalité» et donc la base légale prévue à l'art. 23. Dans le cadre de ses activités de surveillance, la FINMA traite une multitude de données. La surveillance des marchés financiers suppose de disposer d'informations complètes sur les assujettis et sur les acteurs des marchés financiers. Parmi les données traitées figurent aussi des données sensibles. Le but du traitement est en outre susceptible de porter atteinte à des droits fondamentaux, à commencer par la liberté économique. Aussi le Conseil fédéral propose-t-il de modifier la base légale formelle du traitement de données par la FINMA, afin de satisfaire aux exigences de l'art. 30, al. 2, P-LPD. Le traitement de données peut être confié à des agents spécialisés (personnes mandatées par la FINMA au sens de l'art. 14, al. 4, LFINMA et prestataires mandatés sous le régime du droit privé).

De par la nature de sa mission, la FINMA reçoit une multitude de données de la part des institutions surveillées aussi bien que de tiers. Pour qu'elle puisse découvrir dans cette masse de données un éventuel comportement fautif au regard du droit de la surveillance, elle ne peut se dispenser de traiter des données personnelles pour effectuer des profilages. En particulier dans le cadre de la surveillance des marchés (par ex. pour une clarification sur un possible délit d'initié ou une manipulation de marché), la FINMA est confrontée à de très importantes quantités de données relatives aux échanges commerciaux ou aux transactions, qui doivent être exploitées et évaluées de manière automatisée en lien avec les personnes concernées. Pour assurer une surveillance efficiente, la FINMA doit pouvoir traiter les données en question pour un profilage (*al. 3*).

Comme c'est déjà le cas, la FINMA règlera les modalités par voie d'ordonnance (*al. 4*).

Art. 23a Registre public

Cette disposition correspond à l'art. 23, al. 2, du droit en vigueur.

299 RS **956.1**

9.2.69 Loi fédérale du 19 mars 1976 sur la coopération au développement et l'aide humanitaire internationales[300]

Art. 13a, al. 1, phrase introductive et let. g

Vu que le P-LPD abroge la protection des données personnelles des personnes morales, la référence à ces dernières doit être supprimée (cf. ch. 9.1.11).

La notion de «profil de la personnalité» prévue à la let. g est supprimée. Voir le commentaire du ch. 9.2.2.

Il convient de signaler que cette disposition est abrogée dans le cadre de l'avant-projet de révision du Conseil fédéral du 28 juin 2017 de la loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères. (cf. ch. 9.2.13).

9.2.70 Loi du 30 septembre 2016 sur la coopération avec les Etats d'Europe de l'Est[301]

Art. 15, al. 2, phrase introductive

La notion de «profil de la personnalité» est supprimée. Voir le commentaire du ch. 9.2.2.

Il convient de signaler que cette disposition est abrogée dans le cadre de l'avant-projet de révision du Conseil fédéral du 28 juin 2017 de la loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères. (cf. ch. 9.2.13).

9.3 Commentaire des modifications des lois fédérales mettant en œuvre les exigences de la directive (UE) 2016/680

Lorsque la même modification apparaît dans plusieurs textes de lois, elle n'est commentée qu'une seule fois. Ensuite, le texte indique la référence de la première disposition commentée.

9.3.1 Code pénal[302]

Afin de transposer les exigences de la directive (UE) 2016/680, le présent projet prévoit d'introduire un certain nombre de dispositions de protection des données

300 RS **974.0**
301 RS **974.1**
302 RS **311.0**

applicables aux échanges de données effectués dans le domaine de la coopération policière. À l'exception de certaines dispositions spécifiques, ces dispositions s'appliquent non seulement aux autorités fédérales, mais aussi aux autorités cantonales. La Confédération fait ici usage de sa compétence de légiférer, puisque le domaine de la coopération internationale en matière pénale relève du droit fédéral. En effet, lorsque la Constitution attribue à la Confédération la compétence de légiférer dans un certain domaine, le législateur fédéral peut être amené à adopter des dispositions de protection des données, qui s'appliquent également aux autorités cantonales chargées d'exécuter le droit fédéral.

Art. 349a Bases juridiques

Cette disposition met en œuvre les art. 8 et 10 de la directive (UE) 2016/680, qui prévoient en substance qu'un traitement de données tombant dans le champ d'application de cet acte n'est licite que s'il repose sur une base légale ou, à défaut, dans certains cas spécifiques énumérés par les dispositions susmentionnées. A défaut de base légale, les autorités fédérales compétentes ne sont en droit de communiquer des données que dans les cas prévus à l'art. 349*a*, let. a et b. Par contre, elles ne peuvent pas se prévaloir des cas de communication prévus à l'art. 33, al. 2, let. a, b et e, P-LPD, car ils ne sont pas compatibles avec les exigences des art. 8 et 10 de la directive (UE) 2016/680.

Art. 349b Egalité de traitement

Cette disposition met en œuvre l'art. 9, par. 3 et 4, de la directive (UE) 2016/680, qui instaure une égalité de traitement entre les autorités des Etats Schengen et les autorités nationales de poursuite pénale. L'art. 349*b* correspond à la solution retenue par le législateur fédéral à l'art. 6 LEIS. Les communications de données à des autorités d'un Etat Schengen ou à une autorité nationale sont soumises aux mêmes conditions de protection des données. L'adoption de nouvelles restrictions légales reste possible, pour autant que le principe d'égalité soit respecté.

Art. 349c Communication de données personnelles à un Etat tiers ou à un organisme international

Cette disposition met en œuvre les art. 35 à 38 de la directive (UE) 2016/680, qui obligent les Etats Schengen à prévoir que des données personnelles ne peuvent être communiquées à un Etat tiers ou à un organisme international que si certaines conditions cumulatives sont remplies.

L'art. 349*c* s'inspire de la systématique et du contenu des art. 13 et 14 P-LPD, sous réserve de certaines modifications liées aux exigences des art. 35 à 38 de la directive (UE) 2016/680.

Al. 1

L'al. 1 pose le principe selon lequel aucune donnée ne peut être communiquée à l'autorité compétente d'un Etat qui n'est pas lié à la Suisse par l'un des accords d'association à Schengen (Etat tiers) ou à un organisme international si la personna-

lité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'un niveau de protection adéquat. Cette disposition vise uniquement les pays qui ne sont pas liés par un des accords d'association à Schengen.

Al. 2

L'al. 2 définit les cas dans lesquels il y a lieu de considérer que l'Etat tiers ou l'organisme international assure un niveau de protection des données adéquat. Il s'agit d'une liste exhaustive de conditions alternatives. Si l'une de ces conditions est réalisée, il n'existe plus d'obstacle lié à la protection des données pour communiquer des données à un Etat tiers ou à un organisme international.

En vertu de la *let. a*, la législation d'un Etat tiers assure un «niveau de protection des données adéquat» lorsque l'Union européenne l'a constaté par voie de décision. L'organe compétent est la Commission européenne. La décision d'adéquation est rendue conformément à l'art. 36 de la directive (UE) 2016/680. L'al. 2, let. a, se distingue de l'art. 13, al. 1, P-LPD, qui charge le Conseil fédéral d'examiner si l'Etat concerné assure un niveau de protection adéquat. Si une autorité envisage de communiquer des données à un Etat tiers dans le cadre de la coopération policière et judiciaire instaurée par Schengen, elle doit se référer aux décisions d'adéquation de la Commission européenne. Dans les autres domaines, le responsable du traitement se base sur la constatation du Conseil fédéral. Cette différence de régime ne conduit pas en principe à une situation d'insécurité juridique, puisque aujourd'hui déjà le préposé publie une liste des Etats assurant un niveau de protection des données qui correspond essentiellement aux décisions d'adéquation rendues par la Commission européenne.

Les *let. b* et *c* prévoient deux autres cas dans lesquels l'autorité compétente peut considérer que la transmission ne menace pas gravement la personnalité des personnes concernées. Ainsi, une communication de données est licite si le niveau de protection des données est assuré soit par un traité international (let. b) soit par des garanties spécifiques (let. c). L'al. 2, let. b, correspond à la condition prévue à l'art. 13, al. 2, let. a, P-LPD. Par «traité international», on entend non seulement les accords internationaux conclus avec un Etat tiers ou un organisme international dans le domaine de la coopération policière et qui répond aux exigences de la directive (UE) 2016/680 mais aussi toute convention internationale en matière de protection des données à laquelle l'Etat destinataire serait partie. Quant à l'al. 2, let. c, il correspond à la condition de l'art. 13, al. 2, let. c, P-LPD. En vertu de cette disposition, l'autorité compétente peut envisager de communiquer des données à un Etat tiers ou à un organisme international lorsque ceux-ci fournissent des garanties spécifiques qui assurent une protection adéquate de la personne concernée.

Al. 3

Conformément à l'al. 3, si l'autorité compétente est une autorité fédérale, elle doit communiquer au préposé les catégories de communications de données personnelles qui ont été effectuées conformément à l'al. 2, let. c. Il ne s'agit pas d'informer le préposé de chaque communication, mais de lui annoncer quelles sont les catégories de communications qui sont effectuées en vertu de cette disposition. Selon l'al. 3, *2e phrase*, chaque communication est documentée. Cette documentation permet au

préposé de procéder aux vérifications nécessaires et de prononcer, le cas échéant, une interdiction en vertu de l'art. 45, al. 2, P-LPD.

Al. 4 et 5

Si le niveau de protection adéquat des données ne peut pas être assuré conformément à l'al. 2, l'al. 4 prévoit une liste exhaustive d'exceptions. Si une de ces exceptions s'applique, l'autorité est libérée de l'interdiction de communiquer des données personnelles à un Etat tiers ou à un organisme international n'assurant pas un niveau de protection adéquat. Cette disposition transpose les exigences de l'art. 38 de la directive (UE) 2016/680. Comme il ressort du considérant 72 de l'acte européen, ces dérogations devraient être interprétées de manière restrictive et ne devraient pas permettre des transferts fréquents, massifs et structurels de données ni des transferts de données à grande échelle mais des transferts qui devraient être limités aux données strictement nécessaires.

L'al. 4, *let. a*, dispose que des données personnelles peuvent être communiquées dans un cas d'espèce si la communication est nécessaire pour protéger la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers. En vertu de la *let. b*, une communication est également envisageable lorsqu'en l'espèce elle est nécessaire pour prévenir un danger immédiat ou sérieux pour la sécurité publique d'un Etat Schengen ou d'un Etat tiers.

L'al. 4, *let. c* et *d*, prévoit deux autres exceptions. Celles-ci ne sont toutefois applicables que si aucun intérêt digne de protection prépondérant de la personne concernée ne s'oppose à la communication. Les termes «prévenir, constater et poursuivre une infraction» correspondent au champ d'application de la directive (UE) 2016/680, qui règle la protection des personnes physiques à l'égard des traitements des données «à des fins de prévention et de détection des infractions, d'enquêtes et de poursuite en la matière». Dans le cadre des let. c et d, l'autorité doit donc procéder à une pesée des intérêts pour déterminer lequel de l'intérêt public menacé ou de l'intérêt de la personne concernée prévaut. L'autorité doit renoncer à se prévaloir des exceptions prévues aux let. c et d si elle arrive à la conclusion que l'intérêt digne de protection de la personne concernée prime les intérêts de la poursuite pénale, lorsque par exemple la communication pourrait mettre en danger la vie de la personne concernée. Si l'autorité compétente est une autorité fédérale, elle doit communiquer au préposé les communications effectuées en vertu de l'al. 4 (*al. 5*).

Art. 349d Communication de données personnelles provenant d'un Etat Schengen à un Etat tiers ou à un organisme international

Cette disposition met en œuvre les exigences de l'art. 35, par. 1, let. c et e, et 2, de la directive (UE) 2016/680, qui prévoit une obligation pour les Etats Schengen de faire en sorte que les données reçues d'un Etat Schengen ne puissent être communiquées à un Etat tiers ou à un organisme international que si certaines conditions cumulatives sont remplies. Cette disposition s'applique aux autorités suisses qui ont reçu des données d'un Etat Schengen dans le cadre d'une procédure de coopération policière et qui envisagent de les communiquer à un Etat tiers ou à un organisme international en vue de les assister. Sous réserve de quelques modifications, l'art. 349*d* correspond à l'art. 6*b* LEIS qui est supprimé pour des raisons de systématique.

Une communication n'est envisageable que si les trois conditions cumulatives de l'*al. 1* sont remplies. Conformément aux principes de finalité et de proportionnalité, la communication doit permettre la prévention, la constatation ou la poursuite d'une infraction et l'autorité destinataire doit être compétente en la matière (*phrase introductive* et *let. a*). L'Etat Schengen auprès duquel les données ont été collectées doit de plus donner préalablement son accord (*let. b*). Enfin, l'Etat tiers ou l'organisme international doit assurer un niveau de protection adéquat au sens de l'art. 349*c* (*let. c*).

L'*al. 2* prévoit une exception à l'obligation d'obtenir l'accord préalable de l'Etat Schengen qui a collecté les données. En vertu des *let. a* et *b*, des données peuvent être communiquées dans un cas d'espèce si l'accord préalable de l'Etat concerné ne peut pas être obtenu en temps utile et si la communication est indispensable pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un Etat Schengen ou d'un Etat tiers ou pour protéger les intérêts essentiels d'un Etat Schengen. Il s'agit de conditions cumulatives. Lorsque des données sont communiquées en vertu de l'al. 2, l'autorité compétente doit en informer sans délai l'Etat Schengen concerné (*al. 3*).

Art. 349e Communication de données personnelles à un destinataire établi dans un Etat tiers

Cette disposition met en œuvre l'art. 39 de la directive (UE) 2016/680, qui autorise les Etats Schengen à prévoir que dans certains cas exceptionnels les autorités compétentes peuvent communiquer des données personnelles directement à un destinataire établi dans un Etat tiers, à certaines conditions. Cette norme vise des cas où il est urgent de transférer des données à l'étranger, par exemple pour sauver la vie d'une personne qui risque d'être la victime d'une infraction ou pour éviter la commission imminente d'un crime ou d'un acte de terrorisme[303].

Selon la définition de l'art. 3, par. 10, de la directive (UE) 2016/680, on entend par «destinataire» une personne physique ou morale, une autorité publique ou tout autre organisme qui reçoit communication des données.

Al. 1

En vertu de l'al. 1, une communication de données personnelles à un destinataire établi dans un Etat tiers ne peut être envisagée que si trois conditions cumulatives sont remplies. Les communications de données en vertu de l'art. 349*e* doivent rester des cas exceptionnels.

La première condition figure dans la *phrase introductive* de l'al. 1. L'autorité compétente doit d'abord constater qu'une communication par les voies habituelles de la coopération policière avec l'autorité compétente de l'Etat tiers concerné ne peut pas être effectuée de manière appropriée en raison notamment d'une situation urgente.

La deuxième condition (*let. a*) prescrit quant à elle que la communication doit être indispensable à l'accomplissement d'une tâche légale de l'autorité compétente, c'est-à-dire une tâche relevant de la prévention, de la constatation ou de la poursuite

303 Consid. 73 de la directive (UE) 2016/680.

d'une infraction. La communication doit en outre être indispensable. Le recours à l'art. 349*e* ne doit dès lors pas constituer une solution de facilité pour l'autorité compétente. La communication n'est indispensable que si elle est une condition *sine qua non* pour l'accomplissement de la tâche légale de l'autorité.

Enfin, aucun intérêt digne de protection prépondérant de la personne concernée ne doit s'opposer à la communication envisagée (*let. b*). L'autorité doit donc procéder à une pesée des intérêts pour déterminer lequel de l'intérêt public menacé ou de l'intérêt de la personne concernée prévaut.

Al. 2

L'al. 2 prescrit que l'autorité compétente communique les données personnelles au destinataire avec l'interdiction expresse de les utiliser pour d'autres finalités que celles qu'elle a fixées. Il s'agit d'une concrétisation du principe de finalité.

Al. 3

En vertu de l'al. 3, l'autorité compétente doit informer immédiatement l'autorité compétente de l'Etat tiers de toute communication de données personnelles, pour autant que cette information soit jugée appropriée. Elle n'est pas tenue de le faire si elle a par exemple connaissance de cas de violations des droits de l'homme qui auraient été commises par l'autorité compétente de l'Etat tiers concerné (consid. 73 de la directive [UE] 2016/680).

Al. 4 et 5

L'al. 4 dispose que si l'autorité compétente est une autorité fédérale, elle doit en outre informer immédiatement le préposé de toute communication de donnés effectuée en vertu de l'art. 349*e*. Contrairement à l'obligation prévue à l'art. 349*c*, al. 4, le préposé doit être informé de chaque communication et non pas seulement des catégories de communications qui auraient été effectuées. Les communications doivent en outre être documentées (al. 5). Cette documentation permet au préposé de procéder aux vérifications nécessaires et de prononcer le cas échéant une interdiction en vertu de l'art. 45, al. 2, P-LPD.

Art. 349f Exactitude des données personnelles

Les al. 1, 2 et 5 mettent en œuvre l'art. 7, par. 2 et 3, de la directive (UE) 2016/680, qui prévoit en substance que les autorités doivent vérifier l'exactitude des données avant leur transmission et fournir, dans la mesure du possible, des informations permettant à l'autorité destinataire de juger de l'exactitude des données.

L'*al. 1* s'inspire de l'art. 98, al. 1, CPP, qui prescrit que les autorités pénales compétentes rectifient les données personnelles inexactes.

L'*al. 2* reprend la règle prévue à l'art. 98, al. 2, CPP, en précisant qu'en cas de rectification de données inexactes l'autorité compétente ne doit pas seulement informer l'autorité destinataire à laquelle des données inexactes ont été transmises mais aussi l'autorité dont proviennent les données.

L'*al. 3* correspond à l'art. 12 OLPD.

L'*al. 4*, *let. a*, met en œuvre l'art. 6 de la directive (UE) 2016/680, qui oblige le responsable du traitement à établir, dans la mesure du possible, une distinction par rapport aux données des différentes catégories de personnes concernées. Cette disposition tient compte de la problématique liée au changement de catégorie des personnes concernées qui peut intervenir avec l'avancement de la procédure. En effet, selon le considérant 31 de ladite directive, le traitement de données dans les domaines de la coopération judiciaire et policière implique nécessairement différentes catégories de personnes concernées, qu'il convient de distinguer dans la mesure du possible. La phrase introductive de l'al. 4 laisse une certaine marge de manœuvre à l'autorité compétente. Il est possible que dans certains cas cette distinction ne soit pas possible, par exemple lorsque l'état de fait ne permet pas encore de déterminer si une personne est un témoin de l'infraction ou si elle y a participé en tant qu'auteur ou en tant que complice.

L'al. 4, *let. b*, met en œuvre l'art. 7, par. 1, de la directive (UE) 2016/680, qui prévoit que les données fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles[304].

L'*al. 5* délie l'autorité de son devoir d'informer le destinataire lorsque les informations prévues aux al. 2 ou 3 ressortent des données personnelles elles-mêmes ou des circonstances. Cette disposition s'inspire de la solution prévue à l'art. 12 OLPD.

Art. 349g Vérification de la licéité du traitement

Cette disposition met en œuvre l'art. 17 de la directive (UE) 2016/680, qui oblige les Etats Schengen à prévoir un droit pour la personne concernée de demander à l'autorité de contrôle en matière de protection des données de vérifier la licéité d'un traitement de données la concernant, en cas de restriction du devoir d'information ou du droit de la personne concernée à demander l'accès à ses données, la limitation de leur traitement ou la rectification ou l'effacement des données la concernant. La réglementation de l'art. 349*g* s'inspire de la solution prévue à l'art. 8 LSIP avec les modifications qui y sont apportées par le présent projet (voir ci-après ch. 9.3.7).

L'*al. 1* prescrit que la personne concernée peut, dans les cas prévus aux *let. a* à *c*, requérir du préposé qu'il vérifie si les éventuelles données la concernant sont traitées licitement. En raison de la systématique du titre 4 du livre 3 du CP, la personne concernée ne peut se prévaloir de l'art. 349*g* que pour les traitements de données tombant dans le champ d'application du titre 4, à savoir l'entraide en matière de police ou, en d'autres termes, dans le domaine de la coopération policière internationale. De plus, une vérification ne peut être requise que si l'organe fédéral responsable est assujetti à la surveillance du préposé (*al. 2*). Tel est le cas par exemple de fedpol ou de la police judiciaire fédérale.

Le préposé doit communiquer à la personne concernée les résultats de sa vérification de manière toujours identique, à savoir selon le libellé défini à l'al. 3. La communication n'est pas susceptible de recours (*al. 5*).

304 Consid. 30 de la directive (UE) 2016/680.

Si le préposé décide d'ouvrir une enquête contre l'autorité fédérale, la personne concernée n'est pas partie à la procédure (art. 46, al. 2, P-LPD a contrario). Elle ne peut donc pas recourir contre les éventuelles mesures administratives prononcées par le préposé (art. 45 P-LPD).

Art. 349h Enquête

Cette disposition met en œuvre les art. 52 et 53 de la directive (UE) 2016/680, qui obligent les Etats Schengen à prévoir un droit pour la personne concernée d'introduire une réclamation auprès de l'autorité de contrôle en matière de protection des données et de former, le cas échéant, un recours contre la décision de ladite autorité.

L'art. 43, al. 1, P-LPD prévoit que le préposé peut, d'office ou sur dénonciation, ouvrir une enquête contre un organe fédéral si des indices font penser qu'un traitement de données pourrait être contraire à des dispositions de protection des données. La personne concernée peut être le dénonciateur, mais elle n'a pas qualité de partie à la procédure (art. 43, al. 4 *a contrario* et art. 46, P-LPD). Dans la mesure où la Suisse est tenue de reprendre et de mettre en œuvre les exigences de la directive (UE) 2016/680, il y a lieu d'introduire une exception à ce principe, mais uniquement par rapport aux traitements de données effectués par une autorité fédérale dans le cadre d'une procédure de coopération policière. En vertu de l'art. 349*h*, *al. 1*, la personne concernée peut dès lors demander au préposé d'ouvrir une enquête. Pour que sa requête soit recevable, la personne concernée doit rendre vraisemblable qu'un échange de données la concernant est contraire à des normes de protection des données, par exemple par rapport aux exigences applicables aux communications de données à un Etat tiers ou à un organisme international (art. 349*c* P-CP). Si la personne concernée n'est pas en mesure de rendre vraisemblable la violation, le préposé est en droit de déclarer la requête irrecevable. L'*al. 2* précise que la personne concernée ne peut requérir une enquête qu'à l'encontre d'une autorité fédérale assujettie à la surveillance du préposé (cf. commentaire de l'art. 349*g*, al. 2, P-CP). Le cas échéant, le préposé peut prendre des mesures provisoires ou administratives contre l'autorité fédérale concernée (art. 44 et 45 P-LPD). Le préposé doit notifier sa décision à l'autorité fédérale concernée ainsi qu'à la personne concernée, en leur indiquant les voies de recours.

Art. 355a, al. 4

L'al. 4 est nouveau. Il précise que les échanges de données personnelles avec Europol sont assimilés à un échange avec une autorité compétente d'un Etat Schengen (art. 349*b*). Selon le considérant 71 de la directive (UE) 2016/680, les accords de coopération conclus entre Europol et un Etat tiers constituent un critère déterminant pour évaluer le niveau de protection des données dudit Etat. On peut donc partir du principe que le législateur européen considère que les prescriptions d'Europol en matière de protection des données offrent un niveau de protection adéquat.

Art. 355f et 355g

Ces dispositions avaient été introduites lors de la reprise par la Suisse de la décision-cadre 2008/977/JAI.

L'art. 355*f* CP règle la communication de données provenant d'un Etat Schengen à un Etat tiers ou à un organisme international dans le domaine de la coopération judiciaire dans le cadre des accords d'association à Schengen. Cette disposition peut être supprimée. Pour des raisons de systématique, cette catégorie de communications est dorénavant réglée dans le P-EIMP.

Contrairement à la décision 2008/977/JAI, la directive (UE) 2016/680 ne règle plus la communication de données personnelles provenant d'un Etat Schengen à une personne privée. L'art. 355*g* peut être abrogé.

9.3.2 Code de procédure pénale[305]

Art. 95a Traitement de données personnelles

La *let. a* met en œuvre les exigences de l'art. 6 de la directive (UE) 2016/680, qui règle la distinction entre différentes catégories de personnes concernées. Cette disposition tient compte de la problématique liée au changement de catégories des personnes impliquées qui peut intervenir avec l'avancement de la procédure. Selon l'art. 6 de la directive (UE) 2016/680, il s'agit par exemple de distinguer les suspects et les personnes reconnues coupables d'une infraction pénale, les victimes et les personnes à l'égard desquelles certains faits laissent présumer qu'elles pourraient être victimes d'une infraction, ou encore les tiers, tels que les témoins ou les personnes appelées à fournir des renseignements. Pour le législateur européen, cette règle est particulièrement importante pour les traitements de données personnelles effectués dans le cadre de la coopération policière ou judiciaire en matière pénale, qui implique nécessairement le traitement de données concernant différentes catégories de personnes. Comme il ressort du considérant 31 de la directive (UE) 2016/680, cette disposition vise à garantir le droit à la présomption d'innocence (art. 10, al. 1, CPP). La let. a prescrit que l'autorité compétente doit veiller à distinguer dans la mesure du possible les différentes catégories de personnes concernées. Cette dernière dispose d'une certaine marge de manœuvre. Il est en effet possible que dans certains cas cette distinction ne puisse pas être effectuée par exemple lorsque l'état de fait ne permet pas encore de déterminer si une personne est un témoin de l'infraction ou si elle y a participé en tant qu'auteur ou en tant que complice.

La *let. b* transpose les exigences de l'art. 7 de la directive (UE) 2016/680, qui porte sur la distinction entre les données à caractère personnel et la vérification de la qualité des données. Le par. 1 oblige les Etats Schengen à prévoir que les données personnelles fondées sur des faits sont, dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles. Comme il ressort de la systématique de l'art. 7, cette disposition concrétise le principe d'exactitude et ne doit pas être interprétée de manière trop restrictive. En effet, le considérant 30 de la directive (UE) 2016/680 précise que «Dans le cadre des procédures judiciaires les déclarations contenant des données à caractère personnel sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables. Le principe

[305] RS **312.0**

d'exactitude ne devrait par conséquent pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une déclaration a été faite». Les autorités pénales ont toutes pour objectif de rechercher la vérité matérielle pour que la justice pénale puisse être rendue. L'art. 95*a*, let. b, P-CPP vise le même but. Le principe d'exactitude vaut en effet pour tous les types de traitement, dans la mesure où les responsables du traitement ont, tout comme les personnes concernées, un intérêt prépondérant à ce que seules des données actuelles et pertinentes soient traitées. L'art. 143 CPP est un cas d'application de l'art. 95*a*, let. b, P-CPP. Cette norme règle l'exécution de l'audition et prescrit à l'al. 5 que l'autorité pénale doit s'efforcer, par des questions claires et des injonctions, d'obtenir des déclarations complètes et de clarifier les contradictions. Enfin, le Conseil fédéral considère que l'art. 95*a*, let. b, CPP n'a pas de portée sur le jugement d'un tribunal ou sur l'ordonnance pénale d'un ministère public. En effet, lorsque l'autorité de jugement détermine le mobile de l'auteur de l'infraction ou prend en compte sa situation personnelle, sa personnalité ou des circonstances atténuantes, il ne s'agit pas d'appréciations personnelles mais d'éléments faisant partie intégrante de la motivation du jugement, qui n'ont pas à être présentés séparément.

Art. 98, al. 2

L'art. 98 règle le principe d'exactitude.

En ce qui concerne la modification apportée à l'al. 2, voir le commentaire de l'art. 349*f*, al. 2, P-CP (ch. 9.3.1).

9.3.3 Loi du 20 mars 1981 sur l'entraide pénale internationale[306]

Le P-LPD ne s'applique pas aux procédures d'entraide judiciaire (art. 2, al. 3, P-LPD). Le présent projet introduit dès lors dans l'EIMP une nouvelle section 1*b* relative à la protection des données. Ces dispositions mettent en œuvre les exigences de la directive (UE) 2016/680. En effet, les traitements de données personnelles effectués dans le cadre d'une procédure d'entraide judiciaire tombent dans le champ d'application de l'acte européen.

La section 1*b* s'applique non seulement aux autorités fédérales (par ex. l'OFJ ou le Ministère public de la Confédération), mais aussi aux autorités cantonales qui collaborent à une procédure d'entraide judiciaire ou qui sont chargées de statuer sur la demande de coopération de l'Etat étranger (art. 1, al. 1, EIMP). La Confédération fait ici usage de sa compétence de légiférer, puisque le domaine de la coopération internationale en matière pénale relève du droit fédéral.

Les prétentions en matière de protection des données sont tranchées dans le cadre de la procédure d'entraide pendante et suivent les mêmes voies de droit.

306 RS **351.1**

Art. 11b Droit aux renseignements dans le cadre d'une procédure pendante

Cette disposition introduit un droit d'accès aux données personnelles en faveur des personnes visées par une demande de coopération internationale en matière pénale. Elle met en œuvre les exigences de la directive (UE) 2016/680 (art. 14 et 18).

Conformément à l'*al. 1*, les personnes concernées doivent recevoir, en sus des données personnelles les concernant, toutes les informations énumérées aux let. a à e. La personne concernée doit être informée sur la finalité et la base juridique du traitement (*let. a*) ainsi que sur la durée de conservation des données ou, si cela n'est pas possible, les critères pour fixer cette dernière (*let. b*). Elle doit également recevoir des informations sur les destinataires ou catégories de destinataires (*let. c*) ainsi que les informations disponibles sur l'origine des données (*let. d*). Enfin, elle doit recevoir les informations nécessaires à la mise en œuvre de ses droits (*let. e*). L'autorité compétente doit par exemple lui indiquer que ses éventuelles prétentions en matière de protection des données sont tranchées dans le cadre de la procédure d'entraide judiciaire et qu'elles suivent les mêmes voies de droit.

Le droit d'accès de la personne concernée n'est pas absolu. L'*al. 2* prescrit en effet que l'autorité compétente peut refuser, restreindre ou différer la communication en vertu de l'art. 80*b*, al. 2, EIMP ou si l'une des conditions prévues aux *let. a* à *c* est remplie. La décision de l'autorité doit être motivée de telle manière à ne pas divulguer les informations qui font l'objet de son refus.

Art. 11c Restriction du droit d'accès applicable aux demandes d'arrestation en vue d'extradition

Cette disposition introduit une restriction au droit d'accès applicable aux données personnelles traitées dans le cadre de demandes d'arrestation en vue d'extradition. Il s'agit d'un régime dit du «droit d'accès indirect» qui s'inspire de la solution prévue à l'art. 8 LSIP, avec les modifications qui y sont apportées par le présent projet (voir ci-après ch. 9.3.7). L'art. 11*c* tient également compte de l'art. 17 de la directive (UE) 2016/680, qui oblige les Etats Schengen à prévoir un droit pour la personne concernée de demander à l'autorité de contrôle en matière de protection des données de vérifier, en cas de restriction de son droit d'accès, la licéité d'un traitement de données la concernant.

Al. 1

L'al. 1 détermine l'autorité compétente pour répondre à une personne qui souhaite savoir si l'Etat étranger a adressé à la Suisse une demande d'arrestation en vue d'extradition à son encontre. Il s'agit de l'OFJ. Toute autre autorité fédérale ou cantonale saisie d'une telle demande doit la transmettre sans délai à l'office précité.

Al. 2 à 6

Selon l'al. 2, la personne qui demande à l'OFJ si celui-ci a reçu une demande d'arrestation en vue d'extradition d'un Etat étranger reçoit une réponse toujours identique, selon laquelle aucune donnée le concernant n'est traitée illicitement et qu'elle peut demander au préposé si les éventuelles données la concernant sont traitées licitement. La personne intéressée n'est ainsi pas en mesure de savoir s'il

existe une demande d'arrestation en vue d'extradition à son encontre. Aujourd'hui, la situation par rapport au droit d'accès direct de la personne concernée n'est pas satisfaisante. En effet, un tel droit permet en principe à toute personne de savoir si elle est recherchée. S'il est vrai que le droit d'accès peut être refusé, une telle décision doit être motivée. Or le simple fait de refuser l'information peut indiquer au requérant s'il fait l'objet d'une demande d'arrestation en vue d'extradition. Avec l'introduction d'un droit d'accès indirect, le P-EIMP a pour but d'éviter que des personnes recherchées ne puissent savoir dans quels pays elles peuvent se rendre sans risquer de se faire arrêter en vue de leur extradition. Au demeurant, le régime prévu à l'art. 11*c* est de durée limitée. En effet, si la personne concernée est arrêtée en Suisse, elle peut se prévaloir de l'ensemble des droits que lui confère l'EIMP dans le cadre de la procédure d'extradition la concernant.

Comme indiqué ci-dessus, la personne concernée dispose du droit de saisir le préposé pour que ce dernier vérifie la licéité du traitement (al. 2). Cette solution constitue un bon compromis entre l'intérêt de la personne concernée à la protection de sa sphère privée et l'intérêt public à ne pas mettre en péril la poursuite pénale d'un Etat étranger. La réponse du préposé doit toujours avoir la même teneur. Il indique à la personne concernée: soit qu'aucune donnée la concernant n'est traitée illégalement, soit qu'il a constaté une erreur relative au traitement des données personnelles et qu'il a ouvert une enquête conformément à l'art. 43 P-LPD. Cette disposition doit être interprétée et appliquée de la même manière que d'autres droits d'accès indirect prévus en droit fédéral, notamment aux art. 8 LSIP et 18, al. 4, LMSI.

En vertu de l'al. 3, le préposé effectue la vérification demandée. Il se limite à vérifier la licéité du traitement par rapport aux exigences de protection des données, et non par rapport au respect des conditions applicables à la coopération internationale en matière pénale. S'il constate une erreur relative au traitement des données, il peut ordonner à l'OFJ d'y remédier. Tel pourrait être le cas si la sécurité du traitement n'est pas garantie ou si des autorités ou des tiers non autorisés ont accès aux données.

Les al. 3 à 6 coïncident avec les dispositions correspondantes de l'art. 349*g* P-CP (cf. ch. 9.3.1).

Al. 7

Enfin, l'al. 7 prévoit qu'en dérogation à l'al. 2, l'OFJ est habilité à fournir à la personne concernée les renseignements demandés, avec l'accord de l'Etat requérant.

Art. 11d Droits de rectification et d'effacement de données personnelles

Cette disposition règle les droits de rectification et d'effacement de la personne visée par une demande de coopération internationale en matière pénale. Elle met en œuvre les exigences de la directive (UE) 2016/680 (art. 16 et 18).

En vertu de l'*al. 1*, la personne visée par une demande de coopération en matière pénale a le droit d'exiger de l'autorité compétente qu'elle efface ou rectifie les données personnelles la concernant qui sont traitées en violation de l'EIMP, notamment si elles sont inexactes. Elle peut par exemple demander la rectification de données personnelles concernant son identité (nom et prénom, sexe, date de naissance, natio-

nalité, lieu de naissance) et que celles-ci soient complétées. Le principe d'exactitude vaut pour tous les types de traitements, dans la mesure où les autorités ont, tout comme la personne concernée, un intérêt prépondérant à ce que seules des données actuelles et pertinentes soient traitées. La preuve de l'inexactitude des données personnelles incombe à la personne concernée. Le droit de rectification et d'effacement ne vaut toutefois pas pour toutes les données personnelles. En particulier, il n'est pas possible de demander la rectification ou l'effacement du contenu matériel de données personnelles collectées à titre probatoire ou concernant les infractions fondant la demande de coopération dans le cadre d'une procédure d'entraide judicaire. En effet, l'al. 4 prescrit que la vérification de l'exactitude de telles données relève de la compétence de l'autorité pénale étrangère. La personne visée par une demande de coopération ne peut donc pas contester l'exactitude de ces données auprès de l'autorité compétente de l'Etat requis, mais doit le faire, le cas échéant, devant l'autorité compétente de l'Etat requérant.

L'*al. 2* prévoit une mesure moins radicale que l'effacement de données personnelles. Ainsi, en lieu et place de cette mesure, l'autorité compétente doit limiter le traitement des données personnelles si certains conditions remplies. Cette mesure signifie que le traitement de données reste possible, mais uniquement s'il poursuit certaines finalités. Comme il ressort du considérant 47 de la directive (UE) 2016/680, la limitation d'un traitement doit être comprise en ce sens que l'autorité ne peut traiter les données concernées que pour les finalités qui ont empêché leur effacement. L'al. 2 prévoit trois cas de figure.

Selon la *let. a*, l'autorité compétente doit limiter le traitement de données personnelles lorsque l'exactitude des données est contestée par la personne concernée et que ni leur exactitude ni leur inexactitude ne peut être établie. Dans ce cas de figure, la limitation du traitement signifie que l'autorité compétente ne peut traiter les données personnelles litigieuses que dans le but de constater leur exactitude ou leur inexactitude. L'autorité peut par exemple communiquer les données à l'autorité étrangère qui les lui a transmises pour vérification. Une fois l'exactitude des données établie, l'autorité compétente peut en poursuivre le traitement sans autres restrictions. Si par contre les données personnelles s'avèrent inexactes, l'autorité compétente doit les effacer, à moins que les let. b ou c ne s'appliquent au cas d'espèce.

La *let. b* prescrit que l'autorité compétente doit limiter le traitement lorsque la protection d'intérêts prépondérants l'exige, notamment les intérêts mentionnés à l'art. 80*b*, al. 2, EIMP. Ici, l'autorité compétente doit limiter le traitement, en ce sens qu'elle peut continuer à traiter des données personnelles, mais uniquement pour les finalités qui ont empêché leur effacement. Elle est donc en droit de communiquer des données personnelles à l'autorité étrangère pour sauvegarder des intérêts prépondérants.

En vertu de la *let. c*, l'autorité compétente n'est pas non plus tenue d'effacer des données lorsque leur effacement risque de compromettre une procédure de coopération internationale en matière pénale ou la procédure étrangère fondant la demande de coopération en matière pénale. Ici, des données personnelles peuvent être communiquées à une autorité étrangère, dans la mesure où leur effacement constituerait un obstacle au bon déroulement de ces procédures.

L'*al. 3* prescrit que l'autorité compétente informe immédiatement l'autorité qui lui a transmis les données personnelles ou qui les a mises à sa disposition ou à laquelle elles ont été communiquées sur les mesures prises en vertu des al. 1 ou 2.

Enfin, l'*al. 4* prescrit que la vérification de l'exactitude de données personnelles collectées à titre probatoire ou concernant les infractions fondant la demande de coopération en matière pénale relève de la compétence de l'autorité étrangère compétente. La coopération judiciaire internationale en matière pénale vise l'exécution par un Etat de mesures propres visant à faciliter la poursuite et la répression d'infractions pénales dans un autre Etat. Deux procédures sont en cours: d'une part la procédure pénale étrangère, d'autre part la procédure d'entraide judiciaire devant l'autorité compétente. La seconde est au service de la première. L'exactitude des données personnelles collectées à titre probatoire (par ex. des extraits bancaires, des enregistrements ou des procès-verbaux d'audition de témoins) ou concernant les infractions fondant la demande de coopération en matière pénale (par ex. les faits, la qualification des infractions, la qualité de la personne concernée dans le cadre de la procédure pénale) ne saurait être vérifiée par l'autorité compétente de l'Etat requis dans le cadre d'une procédure d'entraide judiciaire. En effet, la procédure pénale étrangère a précisément pour rôle de déterminer si des données personnelles sont exactes ou non. Conformément à la maxime de l'instruction, l'autorité pénale compétente est tenue de rechercher d'office tous les faits pertinents pour la qualification de l'acte et le jugement du prévenu, à la charge ou la décharge de ce dernier. C'est dans ce cadre que l'exactitude des données personnelles collectées à titre probatoire ou concernant les infractions faisant l'objet de la procédure pénale doit être vérifiée.

Art. 11e Egalité de traitement

Cette disposition règle l'égalité de traitement entre les autorités des Etats qui sont liés à la Suisse par l'un des accords d'association à Schengen et les autorités nationales par rapport au régime de protection des données. Elle met en œuvre l'art. 9, par. 3 et 4, de la directive (UE) 2016/680.

L'art. 9, par. 3 et 4, de la directive (UE) 2016/680 doit être interprété en relation avec l'art. 60 de la directive (UE) 2016/680, qui prévoit que les dispositions particulières des actes juridiques de l'Union européenne adoptés avant l'adoption de la directive (UE) 2016/680 et qui règlent le traitement entre Etats membres demeurent inchangées (voir également consid. 94). Cette interprétation préserve ainsi la déclaration commune de la Suisse et de l'Union européenne sur l'art. 23, par. 7, de la convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne[307].

L'art. 11*e* n'a pas d'incidence sur le respect du principe de la spécialité consacré à l'art. 67 EIMP. Selon l'al. 1 de cette disposition, les renseignements et les documents obtenus par voie d'entraide ne peuvent, dans l'Etat requérant, ni être utilisés aux fins d'investigations ni être produits comme moyens de preuve dans une procédure pénale visant une infraction pour laquelle l'entraide est exclue.

307 Accord entre la Confédération suisse, l'Union européenne et la Communauté européenne sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen, conclu le 26 octobre 2004; RS **0.362.31**.

Pour le surplus, voir le commentaire de l'art. 349*b* P-CP (ch. 9.3.1).

Art. 11f Communication de données personnelles à un Etat tiers ou à un organisme international

Cette disposition règle la communication de données à un Etat tiers ou à un organisme international. La teneur de cette disposition correspond en substance à celle de l'art. 349*c* P-CP. Toutefois, contrairement à l'art. 349*c*, al. 3, P-CP, l'art. 11*f* ne prévoit pas une obligation pour les autorités fédérales de communiquer au préposé les catégories de communications de données personnelles effectuées conformément à l'art. 11*f*, al. 2, let. c, ni de l'informer des communications de données personnelles effectuées en vertu de l'al. 3. Cette différence se justifie par le fait que le préposé n'est pas compétent pour surveiller les traitements de données effectués dans le cadre d'une procédure d'entraide judiciaire internationale en matière pénale (cf. commentaire de l'art. 3, al. 2, let. e, P-LPD). Pour le surplus, il y a lieu de se référer par analogie au commentaire relatif à l'art. 349*c* P-CP. (cf. ch. 9.3.1).

Art. 11g Communication de données personnelles provenant d'un Etat Schengen à un Etat tiers ou à un organisme international

Cette disposition règle la communication de données provenant d'un Etat Schengen à un Etat tiers ou à un organisme international. La teneur de cette disposition correspond en substance à celle de l'art. 349*d* P-CP. Toutefois, contrairement à l'art. 349*d*, al. 1, let. a, P-CP, l'art. 11*g*, *al. 1*, *let. a*, vise également l'hypothèse où les données reçues d'un Etat Schengen sont communiquées à un Etat tiers pour exécuter une décision pénale. En effet, ce cas de figure relève de l'entraide judiciaire. Pour le surplus, il y a lieu de se référer par analogie au commentaire relatif à l'art. 349*d* P-CP (cf. commentaire ci-dessus ch. 9.3.1).

Art. 11h Modalités applicables aux communications de données personnelles

Cette disposition règle les modalités applicables aux communications de données personnelles. Elle correspond à l'art. 349*f*, al. 3 à 5, P-CP (cf. commentaire ci-dessus ch. 9.3.1).

9.3.4 Loi fédérale du 22 juin 2001 sur la coopération avec la Cour pénale internationale[308]

Art. 2a Protection des données personnelles

Afin de transposer les exigences de la directive (UE) 2016/680, il est nécessaire d'introduire dans la loi sur la coopération avec la Cour pénale internationale un renvoi aux art. 11*b* à 11*d* et 11*f* à 11*h* P-EIMP. L'art. 11*e* est exclu de ce renvoi car il règle l'égalité de traitement entre autorités Schengen. Il ne s'applique donc pas à la Cour pénale internationale.

308 RS **351.6**

9.3.5 Loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[309]

Art. 9a Protection des données personnelles

Afin de transposer les exigences de la directive (UE) 2016/680, il est nécessaire d'introduire dans la loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale un renvoi aux art. 11*b*, 11*d* et 11*f* à 11*h* P-EIMP.

9.3.6 Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres Etats[310]

Art. 13, al. 2

Dans le cadre de la transposition de la directive (UE) 2016/680, il est nécessaire de modifier l'art. 13, al. 2, en prévoyant un renvoi aux art. 349*a* à 349*h* P-CP.

9.3.7 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[311]

Art. 7, al. 2

L'al. 2 réserve également le nouvel art. 8*a*.

Art. 8 Restriction du droit d'accès applicable au Système de traitement des données relatives aux infractions fédérales

Cet article doit être adapté, puisqu'en vertu de la future LPD le préposé ne rend plus de recommandations mais est habilité à ouvrir une enquête au sens de l'art. 43 P-LPD et à prononcer, le cas échéant, des mesures administratives en vertu des art. 44 et 45.

L'*al. 1* reste inchangé par rapport au droit en vigueur.

L'*al. 2* subit une modification rédactionnelle.

Quant à l'*al. 3*, il est modifié en ce sens que le préposé ne doit plus indiquer à la personne concernée «qu'il a adressé à fedpol la recommandation d'y remédier en vertu de l'art. 27 LPD» mais «qu'il a ouvert une enquête conformément à l'art. 43 LPD».

309 RS **351.93**
310 RS **360**
311 RS **361**

En outre, vu que les art. 44 et 45 P-LPD confèrent des compétences décisionnelles au préposé, l'intervention du Tribunal administratif fédéral telle qu'elle est prévue à la seconde phrase de l'al. 3 peut être supprimée.

L'al. 4 en vigueur peut être abrogé. Le renvoi à l'art. 43 P-LPD est suffisant. Le nouvel *al. 4* prévoit que l'enquête du préposé peut aboutir à une décision (art. 45 P-LPD) contre laquelle fedpol peut recourir.

L'*al. 5* prescrit que les communications visées aux al. 2 et 3 sont toujours libellées de manière identique et ne sont pas motivées. De plus, la communication visée à l'al. 3 n'est pas sujette à recours.

L'*al. 6* reprend l'al. 7 en vigueur, qui reste inchangé.

L'*al. 7* reprend l'al. 8 en vigueur, qui est modifié en ce sens que le préposé peut ordonner – et non plus seulement recommander – à fedpol de fournir à la personne concernée les renseignements demandés si les conditions sont remplies.

Art. 8a Restriction du droit d'accès aux signalements en vue d'une arrestation aux fins d'extradition

Cette disposition introduit une restriction du droit d'accès aux signalements en vue d'une arrestation aux fins d'extradition qui figurent dans un des systèmes énumérés à l'art. 2 LSIP. Si la demande de la personne concernée ne vise pas un de ces systèmes, fedpol est tenu de transmettre la requête à l'OFJ conformément à la règle prévue à l'art. 11*c*, al. 1, P-EIMP.

Pour le surplus, voir le commentaire relatif à l'art. 11*c* P-EIMP (ch. 9.3.3).

9.3.8 Loi fédérale du 12 juin 2009 sur les échanges d'information Schengen[312]

Art. 2, al. 3

Le renvoi aux art. 6 à 6*c* LEIS est remplacé par un renvoi aux art. 349a à h P-CP.

Art. 6a à 6c

Les art. 6*a* à 6*c* ont été introduits dans la LEIS lors de la transposition de la décision-cadre 2008/977/JAI. Afin de diminuer la densité normative du droit fédéral, le Conseil fédéral propose d'abroger ces dispositions et de prévoir un renvoi aux art. 349*a* à 349*h* P-CP.

312 RS **362.2**

10 Entrée en vigueur

Il est prévu que le Conseil fédéral fixe l'entrée en vigueur de la future loi.

Comme indiqué sous ch. 2.2, la Suisse dispose d'un délai maximal de deux ans, à compter de la date de la notification par l'Union européenne, pour reprendre la directive (UE) 2016/680 dans son ordre juridique. Cette directive a été notifiée à la Suisse le 1er août 2016. Par conséquent, le délai maximal pour la reprise et la mise en œuvre de cet acte prend fin le 1er août 2018. S'il est vrai qu'il serait possible de prévoir une entrée en vigueur différée pour les secteurs public et privé, le Conseil fédéral considère qu'une telle solution n'est pas opportune. En effet, le règlement (UE) 2016/679 est applicable à partir du 25 mai 2018 dans les Etats membres de l'Union européenne (art. 99). Il est donc dans l'intérêt de la Suisse que le projet de loi entre en vigueur le plus rapidement possible moyennant certaines dispositions transitoires. De cette manière, le délai de deux ans, qui court en vertu des obligations Schengen de mise en œuvre de la directive (UE) 2016/680, pourra, en principe, être respecté.

11 Conséquences

Les conséquences du projet lui-même et celles de la reprise de la directive sont indissociables et sont ainsi présentées ensemble.

11.1 Conséquences financières et en personnel pour la Confédération

11.1.1 Conséquences financières et en personnel pour le préposé

Le projet de loi introduit toute une série de mesures qui impliquent des tâches nouvelles pour le préposé. Ces mesures sont pour la plupart exigées par le droit européen (à savoir le P-STE 108, la directive [UE] 2016/680 et le règlement [UE] 2016/679) et sont nécessaires pour que la Suisse puisse conserver un niveau de protection des données adéquat par rapport aux standards de l'Union européenne d'une part, et pour qu'elle puisse satisfaire à ses obligations découlant des accords de Schengen d'autre part. Certaines d'entre elles répondent à un besoin de l'économie et visent à faciliter l'application de la loi pour les entreprises. Dans la mesure où de nombreuses entreprises suisses sont susceptibles d'être soumises au règlement (UE) 2016/679, en raison de son champ d'application très large (art. 3), il est important que le projet n'en dévie pas trop. En effet, sans égard à la question de la décision d'adéquation, les entreprises, pour des raisons économiques et de sécurité juridique, doivent pouvoir adopter un comportement et des règles internes sensiblement identiques, qu'elles soient soumises au droit européen ou au droit suisse.

Les nouvelles tâches du préposé entraînent pour lui des besoins supplémentaires en termes de personnel et sur le plan informatique. A cet égard, on peut souligner que l'octroi de ressources suffisantes au préposé constitue un élément important pour

l'Union européenne, tant au niveau de la décision d'adéquation que de la mise en œuvre des acquis de Schengen. L'obligation de doter les autorités de contrôle de ressources suffisantes, élément indispensable à leur indépendance, est en effet prévue par l'ensemble des textes européens (art. 12bis, par. 5, P-STE 108, 42, par. 4, de la directive [UE] 2016/680 et 52, par. 4, du règlement [UE] 2016/679). L'examen du niveau de protection adéquat comprend également un examen de la mise en œuvre effective des mesures. La prochaine évaluation Schengen, qui aura lieu en 2018, portera aussi sur cet aspect. Le groupe des autorités de contrôle pour le SIS II s'est récemment adressé à la Commission européenne, au Parlement européen et au Conseil de l'Union européenne, les appelant à s'assurer que les autorités de contrôle reçoivent effectivement les ressources en personnel et les ressources financières appropriées pour exécuter leurs tâches légales.

11.1.1.1 Besoins en personnel

Les besoins du préposé en personnel supplémentaire ne sont pas statiques, ni linéaires, et sont amenés à évoluer dans le temps. Ainsi par exemple, il est à prévoir qu'au début peu de codes de conduite lui seront soumis, dans la mesure où les branches auront besoin de temps pour les élaborer. Par ailleurs, de nombreuses mesures sont liées entre elles, si bien que les tâches du préposé en lien avec l'une excluront ou limiteront une autre intervention de sa part. S'agissant des codes de conduite par exemple, on peut partir du postulat que la consultation du préposé contribuera à réduire le nombre d'enquêtes en facilitant l'émergence de comportements conformes à la loi. Au final, les tâches de contrôle préventif du préposé contribueront à un meilleur respect de la législation et, partant, à une baisse du nombre d'enquêtes. En conséquence, et afin de coller au plus près de la réalité des besoins du préposé, le Conseil fédéral propose d'une part un octroi échelonné des ressources en personnel (voir le tableau ci-après), et d'autre part une réévaluation des besoins au plus tard cinq ans après l'entrée en vigueur de la loi.

Il est difficile de faire des estimations précises. Pour cette raison, le Conseil fédéral s'est efforcé, pour chaque nouvelle tâche impliquant un besoin en personnel, d'expliciter les hypothèses sous-jacentes qui lui ont permis d'évaluer ce besoin. Cette démarche est également importante eu égard à la réévaluation quinquennale des besoins, car il se pourrait que certains besoins diminuent avec le temps. Dans la mesure du possible, et conformément au principe de la couverture des coûts, les nouveaux postes seront financés par des émoluments (art. 53 P-LPD).

On peut estimer les besoins en personnel du préposé à 10 postes supplémentaires (juristes et informaticiens en classe 24, soit 1 800 000 francs). Ces postes se répartissent de la manière suivante:

– L'art. 10 P-LPD prévoit la possibilité, pour les associations professionnelles et les associations économiques privées ainsi que pour les organes fédéraux, de soumettre leurs *codes de conduite* au préposé. Ce dernier doit prendre position et publier ses prises de position. L'élaboration de codes de conduite par les branches et leur soumission au préposé doivent permettre de favoriser l'autorégulation dans le secteur privé. Ces codes permettront de préciser la

loi et de la mettre en œuvre de manière différenciée selon les secteurs d'activité[313]. Ils répondent à un besoin de sécurité juridique qui a été identifié par l'analyse d'impact de la réglementation (cf. ch.1.8).

A terme, bien que non contraignants, ces codes entraîneront une meilleure application de la loi, et donc des enquêtes moins fréquentes du préposé. Par ailleurs, ceux qui auront soumis leurs codes au préposé seront, à certaines conditions, déchargés du devoir de réaliser une analyse d'impact relative à la protection des données (art. 20, al. 5, P-LPD), ce qui allégera également la charge du préposé, dans la mesure où il ne sera plus impliqué ensuite dans une procédure de consultation préalable (art. 21 P-LPD).

L'encouragement de l'autorégulation est une mesure prévue par le règlement (UE) 2016/679 (art. 40). A la différence du P-LPD, le texte européen prévoit cependant une approbation obligatoire par l'autorité de contrôle, qui confère au code soumis un caractère contraignant pour les responsables du traitement y ayant adhéré. Le Conseil fédéral a renoncé à une telle solution, qui aurait entraîné des coûts plus élevés, dans la mesure où le préposé aurait dû statuer par voie de décision susceptible de recours.

Le nombre de codes qui seront soumis au préposé est estimé à une dizaine par année. La charge de travail y afférente variera selon la complexité et la longueur des codes. En moyenne toutefois, on peut estimer que cette nouvelle tâche occupera une personne à plein temps. Le Conseil fédéral estime qu'il y aura peu de soumissions de codes de conduite la première année, dans la mesure où les branches devront tout d'abord les élaborer. Il estime également que la quantité de codes soumis devrait diminuer avec le temps, le nombre d'organisations habilitées à en édicter n'étant pas illimité. Pour cette raison, il est prévu 0,5 poste pour la première et la cinquième année, et 1 poste entier pour les 2e, 3e et 4e années, étend entendu que durant ces 3 années-ci, le préposé sera plus sollicité.

Ce poste devrait pouvoir être financé à hauteur de 60 % par des émoluments. Le taux de couverture est limité par le fait que le préposé pourra renoncer dans certains cas à la perception d'émoluments, en application de l'art. 3, al. 2, let. a, OGEmol, l'encouragement de l'autorégulation répondant à un intérêt public.

– L'art. 13, al. 2, let. d et e, P-LPD prévoit, pour les communications de données à l'étranger, que les responsables du traitement doivent soumettre pour approbation au préposé les *clauses types de protection des données* et les *règles d'entreprise contraignantes* visant à garantir un niveau de protection adéquat. Cette approbation répond à une exigence du droit européen (art. 12bis, par. 2, let. b, P-STE 108 et 46, par. 2, let b et d, et 47 du règlement [UE] 2016/679). Le préposé devra donc examiner les textes qui lui sont soumis et, le cas échéant, les approuver. Il s'agit d'un élément central pour assurer un niveau de protection approprié des données en regard de la décision d'adéquation de l'Union européenne et des exigences du P-STE 108. Le

313 Pour un exemple, voir le code de l'Union française du marketing du 17 mars 2005: www.cnil.fr/sites/default/files/typo/document/projet-codeUFMD.pdf.

préposé statuera par voie de décision. Ce contrôle préventif du préposé conduira, comme les codes de conduite, à un meilleur respect des normes de protection des données, ce qui devrait, à terme, diminuer le nombre de ses enquêtes.

Le nombre de clauses types et de règles d'entreprise contraignantes qui seront soumises au préposé est estimé à une vingtaine par année. La charge de travail dépendra principalement de la complexité et de la taille des textes. En moyenne, on peut estimer que cette nouvelle tâche occupera une personne à plein temps. Il se pourrait que ce besoin diminue par la suite, dans la mesure où le nombre de règles d'entreprise contraignantes et de clauses types à édicter n'est pas illimité. Ce poste devrait pouvoir être financé à hauteur de 60 % par des émoluments. Ici aussi, le préposé pourra renoncer dans certains cas à percevoir des émoluments, en vertu de l'art. 3, al. 2, let. a, OGEmol).

– L'art. 21 P-LPD prévoit que le préposé doit être consulté lorsqu'une *analyse d'impact relative à la protection de données* (art. 20 P-LPD) montre que le traitement envisagé présenterait un risque élevé pour la personnalité et les droits fondamentaux des personnes concernées si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque. Plus précisément, le préposé doit être consulté lorsque le responsable du traitement estime que ce risque ne peut pas être atténué par des mesures raisonnables au vu des techniques disponibles et des coûts de mise en œuvre. Le devoir de procéder à une analyse d'impact est une exigence du droit européen (art. 8bis, par. 2, P-STE 108, 27 de la directive [UE] 2016/680 et 35 du règlement [UE] 2016/679). La consultation préalable de l'autorité de contrôle en matière de protection des données est expressément prévue par la directive (UE) 680/2016 (art. 28) et le règlement (UE) 679/2016 (art. 36).

  Cette nouvelle tâche impliquera que le préposé examine en détail les analyses d'impact qui lui sont soumises, les traitements de données envisagés, ainsi que les mesures proposées par les responsables du traitement. Le préposé devra ensuite prendre position, dans un délai de deux mois (prolongeable d'un mois). S'il a des objections, il doit proposer des mesures appropriées. Il s'agit d'un exercice contraignant, souvent complexe, qui nécessite l'implication d'un juriste et d'un informaticien. Avec le développement de l'économie digitale, les traitements présentant des risques élevés pour la personnalité et les droits fondamentaux des personnes concernées ont tendance à augmenter et à se complexifier, si bien que l'instrument de l'analyse d'impact va gagner en importance.

  Le nombre d'examens est estimé à une dizaine, voire une quinzaine, par année. Cette nouvelle tâche nécessite 3 postes supplémentaires. Compte tenu du fait que l'art. 21 P-LPD ne sera applicable pendant les deux ans suivant l'entrée en vigueur de la loi que pour les traitements au sens des art. 1 et 2 de la directive 2016/680 (art. 63, al. 2, P-LPD), le Conseil fédéral propose que 2 des 3 postes supplémentaires pour l'examen des analyses d'impact soient créés à l'échéance de ce délai. La création d'un poste dès l'entrée en vigueur de la loi est justifiée par le fait que le préposé doit mettre en place les procédures internes nécessaires à cette tâche inédite, de façon à être opé-

rationnel le moment venu (informatique, directives). Par ailleurs, un grand travail de sensibilisation auprès des responsables du traitement devra être effectué, compte tenu de la complexité de l'instrument de l'analyse d'impact. Cette mesure devrait elle aussi à terme conduire à une bonne application de la loi et mener ainsi à une réduction du nombre d'enquêtes par le préposé. Ces postes devraient pouvoir être financés presque entièrement par des émoluments.

– Le préposé devra désormais ouvrir une *enquête* en présence d'indices suffisants de violation des dispositions de protection des données, alors que selon le droit en vigueur les cas dans lesquels le préposé ouvre une enquête sont limités (art. 29 LPD). Il pourra y renoncer dans les cas de peu d'importance (art. 43, al. 2, P-LPD). Par ailleurs, alors qu'il ne peut aujourd'hui émettre que des recommandations, il pourra à l'avenir rendre des *décisions contraignantes* et, par exemple, interdire lui-même un traitement de données (art. 43 ss P-LPD). Il devra également examiner les annonces de violation de la sécurité des données au sens de l'art. 22 P-LPD. Ces nouvelles compétences sont exigées par le droit européen (art. 7, par. 2, et 12bis, par. 2, let. a et c, P-STE 108, 30 et 47 de la directive [UE] 2016/680, ainsi que 33 et 58, par. 1, let. b, et 2, du règlement [UE] 2016/679) et sont ainsi très importantes, tant en regard de la décision d'adéquation et du respect des exigences du P-STE 108, que de la reprise des exigences de la directive (UE) 2016/680. On rappellera ici que la Suisse, lors de l'évaluation Schengen de 2014 (cf. ch. 1.2.2.3), a déjà reçu une recommandation des experts européens, l'invitant à conférer au préposé des compétences décisionnelles.

  Le préposé aura encore d'autres devoirs en matière de surveillance, prévus dans le cadre de la coopération pénale instaurée par Schengen. Il devra ainsi vérifier notamment la licéité des traitements de données personnelles effectués, sur demande des personnes concernées en cas de restriction de leurs droits (art. 349*g* P-CPP et 11*c* P-EIMP).

  Le nombre d'enquêtes que le préposé devra mener est estimé à une quinzaine, voire une vingtaine. Les annonces de violation de la sécurité des données sont quant à elles estimées entre cinq et dix par an. Ces nouvelles tâches impliquent la création de 3 postes, soit d'une équipe interdisciplinaire composée de deux juristes et d'un informaticien. Selon le Conseil fédéral, ces besoins pourraient diminuer après quelques années. En effet, on peut tabler sur le fait qu'avec le temps, les responsables du traitement connaîtront les règles applicables et s'y conformeront plus naturellement. Par ailleurs, les décisions prononcées par le préposé, de même que les éventuelles sanctions pénales prononcées par les autorités cantonales, devraient avoir un effet incitatif positif. Pour cette raison, le Conseil fédéral propose de passer de 3 à 2,5 postes après quatre ans (soit en 2022–2023).

  S'agissant de mesures de surveillance proprement dites, ces postes ne pourront être financés qu'à raison de 30 % par les émoluments. Le Conseil fédéral précise ici qu'il a renoncé à introduire un système de sanctions administratives, qui aurait nécessité plus de ressources, compte tenu des garanties de procédure supplémentaires qui se seraient dès lors appliquées.

– L'art. 49 P-LPD règle l'*assistance administrative* entre le préposé et les autorités de contrôle en matière de protection des données étrangères. Compte tenu de l'internationalisation croissante des traitements de données, la coopération entre les autorités nationales de protection des données est indispensable. Il s'agit d'ailleurs d'une exigence du droit européen (art. 12bis, par. 7, et 13 ss P-STE 108, 46, par. 1, let. h, et 50 de la directive [UE] 680/2016 et 57, par. 1, let. g, et 61 du règlement [UE] 2016/679). On peut estimer le besoin supplémentaire en personnel à 1 poste. Il n'est pas prévu d'autofinancement pour cette tâche.

– Enfin, le nouveau «bouclier de sécurité» entre la Suisse et les Etats-Unis («*Swiss-US Privacy Shield*», cf. ch. 5 ci-dessus) nécessitera également des ressources supplémentaires. Les conséquences financières pour le préposé dans ce domaine ont déjà été annoncées au Conseil fédéral lorsque ce dernier a pris connaissance, le 11 janvier 2017, du nouveau cadre pour le transfert des données personnelles de la Suisse vers des entreprises sises aux Etats-Unis.

  Le bouclier de sécurité implique, pour le préposé, certaines obligations de coopération. Il transmet les plaintes des personnes concernées à la *Federal Trade Commission*, au Département américain du commerce et à l'*Ombudsperson* du Département d'Etat. Le préposé transmet également les demandes de renseignements à l'*Ombudsperson* du Département d'Etat. Du fait de la forte progression du volume d'externalisation de traitements de données aux Etats-Unis et de l'utilisation aujourd'hui très répandue en Suisse de services de sociétés américaines telles que Facebook, Google ou Apple, on peut s'attendre à une multiplication des plaintes et des demandes de renseignements à traiter par le préposé. Les entreprises certifiées selon le *Swiss-US Privacy Shield* doivent travailler avec le préposé dans deux hypothèses. Premièrement, celles qui traitent des données de ressources humaines des entreprises suisses doivent toujours collaborer avec le préposé pour les affaires relatives à la protection des données. Cette forme de collaboration peut aussi, et c'est la deuxième hypothèse, être librement choisie par les entreprises, en dehors des traitements de données de ressources humaines.

  Pour terminer, le préposé devra désormais vérifier chaque année la qualité des mesures de protection des droits de la personnalité des personnes concernées convenues dans le *Swiss-US Privacy Shield*, en collaboration avec le SECO, et établir un compte rendu.

  On peut estimer le besoin en personnel supplémentaire à 1 poste. Ce dernier ne sera pas être financé par des émoluments.

Les charges supplémentaires en personnel ne peuvent pas être compensées à l'interne, ce d'autant plus que les tâches du préposé n'ont cessé d'augmenter avec le développement exponentiel du numérique, indépendamment même du projet de révision. Par ailleurs, la réduction des tâches du préposé du fait de l'abandon de l'obligation de déclarer les fichiers dans le secteur privé est négligeable.

Comme mentionné en introduction, les besoins en personnel du préposé sont amenés à évoluer dans le temps, selon la tâche envisagée. Le tableau ci-dessous permet de

visualiser cette dynamique en montrant les besoins selon les années. Ces besoins seront réévalués en 2023 au plus tard. Par ailleurs, afin d'avoir une vue d'ensemble, le tableau ci-dessous englobe également les besoins en personnel de l'OFJ (pour les détails, cf. ch. 11.1.2).

	2018–19	2019–20	2020–21	2021–22	2022–23	Financé par des émoluments
Examen des codes de conduite	0,5	1	1	1	0,5	~ 60 %
Approbation des clauses types et des règles d'entreprises contraignantes	1	1	1	1	1	~ 60 %
Examen des analyses d'impact	1	1	3	3	3	~ 90 %
Enquêtes / Examen des annonces de violations de la sécurité des données	3	3	3	3	2,5	~ 30 %
Assistance administrative	1	1	1	1	1	–
Tâches dans le cadre du Swiss-US Privacy Shield	1	1	1	1	1	–
Total postes préposé	7,5	8	10	10	9	
Total postes OFJ	1	1	1	1	1	
Total global	**8,5**	**9**	**11**	**11**	**10**	

11.1.1.2 Besoins en matière informatique

Eu égard à son indépendance, le préposé a besoin d'un budget minimum axé sur l'accomplissement de sa mission, pour couvrir ses frais d'investissement et d'exploitation informatiques. Afin de garantir une exploitation aussi efficace et rentable que possible, il recourt déjà aux services d'assistance (informatique, finances, personnel, logistique) de la Chancellerie fédérale. Il a par ailleurs décidé de recourir aux prestations informatiques standard de la Confédération. En optant pour ces solutions, le préposé contribue à un accomplissement des tâches rentable, sans que son indépendance ne soit remise en cause. Malgré ces efforts, son budget actuel de quelque 300 000 francs au titre des biens et services liés à l'informatique ne lui suffira pas pour mettre en œuvre la nouvelle LPD.

Comme l'économie, l'administration fédérale exploite et développe un grand nombre d'applications qui traitent des quantités importantes de données. Le préposé doit par conséquent s'assurer que les données personnelles soient anonymisées ou pseudonymisées d'une manière qui exclue avec une vraisemblance suffisante, dans l'état actuel de la technique, toute reconstitution de l'identité des personnes. Les applications modernes de traitement de données personnelles ne sont plus aujourd'hui fournies pour une installation locale; elles sont rendues accessibles par Internet. Le

développement du numérique oblige le préposé à effectuer ses clarifications concernant une éventuelle violation de la protection des données d'une manière plus dynamique et ses contrôles d'une manière plus rapide, dans des circonstances plus difficiles.

Face à l'essor du numérique, le préposé a besoin de moyens informatiques supplémentaires pour pouvoir accomplir ses nouvelles tâches:

Tâche	Investissements informatiques	Exploitation, maintenance, assistance, gestion des mises à jour informatiques	Expertise externe, questions spécifiques
	2019	*par an dès* 2020	par an dès 2019
Tests d'infrastructure et de systèmes: Servent à vérifier si le traitement de données effectué par les entreprises et les administrations relève ou non du droit de la protection des données	200 000.–	105 000.–	
Recours à des spécialistes externes: Recours focalisé à des experts informatiques externes compte tenu de la collecte et du traitement accrus et de l'échange de données concernant des personnes			60 000.–
Développement des moyens de travail et de communication électroniques (applications web) pour le renseignement et le conseil	240 000.–	85 000.–	
Total des dépenses informatiques uniques	440 000.–		
Charges informatiques annuelles		190 000.–	60 000.–

Il faut acquérir des systèmes tests afin de vérifier si le traitement de données effectué par les entreprises et les administrations relève ou non du droit de la protection des données. L'analyse devra se concentrer sur les services, les produits et les processus commerciaux à fort potentiel de risque pour la sphère privée. Cela nécessitera des mesures de protection spéciales, raison pour laquelle ces examens auront lieu dans un environnement virtuel sécurisé via un accès Internet normal. On pourra ainsi suivre, notamment, les échanges de données des applications et des produits sur Internet (portails web, intégration de réseaux sociaux et *webtracking* sur des sites Internet, traitement de données sur des appareils mobiles, par ex.).

Du fait de l'augmentation des exigences techniques concernant la protection des données et de la multiplication des appareils mobiles qui collectent des données au moyen de capteurs pour les transmettre à des centres informatiques par Internet, l'autorité de protection des données de la Confédération va devoir recourir au savoir d'experts externes. Vu le dynamisme des technologies de communication et d'information, il ne serait pas utile d'élaborer et d'entretenir activement un savoir spécifique. Bien que l'implication de spécialistes soit nécessaire pour des clarifications individuelles, il n'est pas possible de procéder à l'externalisation générale des clarifications, en raison de la confidentialité de ces opérations.

Le développement des moyens de travail et de communication électroniques (applications web) doit permettre à l'autorité de surveillance des données de la Confédération d'agir de manière préventive et consultative selon les nouvelles prescriptions légales. En font notamment partie la cyberassistance en matière d'analyses d'impact de la protection des données, la saisie et le traitement de messages dénonçant une atteinte à la sécurité des données ou des garanties en cas d'échange de données personnelles avec l'étranger, et les outils interactifs de promotion des règles de comportement conformes à la protection des données. Il faut aussi mettre en place un système d'alerte (systèmes de notification ou registres des traitements de données, par ex.) permettant de dénoncer (y compris de façon anonyme) les violations des prescriptions en matière de protection des données. On reprendra dans la mesure du possible les solutions et les logiciels disponibles dans l'administration fédérale.

L'investissement unique nécessaire sur le plan informatique pour la mise en œuvre de la nouvelle LPD, coûts de projet compris, est aujourd'hui estimé à 440 000 francs. L'acquisition de nouvelles infrastructures et applications entraînera des frais informatiques supplémentaires de 105 000 francs par an. Les frais annuels supplémentaires engendrés par le recours à des spécialistes en informatique est de 60 000 francs.

Les nouvelles solutions devront être élaborées et mises en œuvre d'ici à 2020. Elles devront être renouvelées au bout de cinq ans.

11.1.2 Conséquences financières et en personnel pour l'OFJ

L'examen du niveau de protection des données personnelles d'un Etat étranger ou d'un organisme international (art. 13, al. 1, P-LPD) relèvera de la compétence de l'OFJ. Ce dernier devra non seulement examiner l'existence d'une législation – respectivement d'une réglementation interne – présentant un niveau de protection adéquat, mais également la façon dont elle est mise en œuvre. Il s'agira notamment d'examiner les textes législatifs, la jurisprudence et la doctrine topiques. Des voyages ponctuels à l'étranger sont aussi à prévoir, de même qu'une collaboration avec d'autres autorités, telles que la Commission européenne ou le comité conventionnel de la convention STE 108 modernisée.

Le Conseil fédéral estime que cette nouvelle tâche nécessite 1 poste supplémentaire (un juriste en classe 25). Cela correspond à un coût annuel en personnel de 192 900 francs, y compris les cotisations de l'employeur. Ces coûts ne pourront pas être financés à l'interne. En revanche, les frais relatifs à l'aménagement d'une place

de travail seront compensés. Il faut encore ajouter 50 000 francs à titre de frais professionnels et de mandats d'experts.

Pour son examen, le Conseil fédéral s'appuiera dans la mesure du possible sur les sources disponibles (en particulier les évaluations effectuées dans le cadre de la convention STE 108 ou de l'Union européenne). Néanmoins, le nombre d'Etats à évaluer devrait augmenter à l'avenir, et il s'agit d'un processus dynamique qui ne doit pas être sous-estimé. Par ailleurs, la liste publiée par le Conseil fédéral acquerra une force nouvelle et ce dernier endossera la responsabilité de l'évaluation s'agissant du niveau de protection adéquat des Etats évalués.

11.2 Conséquences pour les cantons et les communes

La ratification par la Suisse du protocole d'amendement de la convention STE 108 lie également les cantons. Les dispositions de cet acte doivent être transposées, si besoin est, conformément à la répartition constitutionnelle des compétences prévues en droit interne. La situation est la même s'agissant de la reprise de la directive (UE) 2016/680.

Des conséquences supplémentaires pour les cantons peuvent résulter du fait que, dans le cadre de la mise en œuvre de la nouvelle loi, le préposé peut faire appel aux organes de police cantonaux et communaux pour l'exécution de ses mesures d'investigation. Une assistance administrative entre le préposé et les autorités cantonales de protection des données est également prévue.

Le renforcement des dispositions pénales, en particulier l'introduction d'une infraction pour insoumission à une décision du préposé, ne devrait pas entraîner d'augmentation importante des procédures pénales cantonales. En effet, les décisions du préposé sont susceptibles de recours. Une fois les décisions entrées en force, leur non-respect devrait se limiter à quelques cas isolés.

11.3 Conséquences dans le secteur informatique

Le projet de loi a un certain nombre de conséquences sur les traitements automatisés de données. Le responsable du traitement doit notamment garantir l'information de la personne concernée lors de tout traitement de données la concernant, notamment sur Internet ou lorsqu'il prend une décision individuelle automatisée à l'encontre de la personne concernée. En outre, s'il envisage d'effectuer des traitements présentant certains risques, il doit procéder à une analyse d'impact relative à la protection des données personnelles et communiquer les risques et les mesures envisagées au préposé. Le responsable du traitement est de plus tenu de prendre les mesures appropriées permettant de mettre en œuvre le principe de protection des données dès la conception et par défaut et de tenir un registre de ses activités de traitements. Enfin, il doit annoncer au préposé et, le cas échéant, également à la personne concernée certains cas de violation de la sécurité des données personnelles.

Les conséquences informatiques pour les organes fédéraux sont plus limitées à différents égards. Ainsi, les obligations d'établir une analyse d'impact relative à la protection des données et de respecter le principe de protection des données dès la conception et par défaut ont peu de conséquences en pratique, puisque l'organe fédéral est déjà tenu aujourd'hui d'annoncer à son conseiller à la protection des données ou, à défaut, au préposé, tout projet de traitement automatisé de données personnelles, afin que les exigences de la protection des données soient immédiatement prises en considération (art. 20, al. 2, OLPD).

L'art. 25 de la directive (UE) 2016/680 oblige les Etats Schengen à prévoir une obligation d'établir des journaux pour certaines opérations de traitement dans des systèmes automatisés. Selon cette disposition, la journalisation doit permettre de déterminer les opérations de traitement effectuées et d'établir le motif, la date et l'heure d'une consultation ou d'une communication de données personnelles, ainsi que, dans la mesure du possible, l'identité de la personne qui a communiqué ou consulté les données et celle des destinataires. Le Conseil fédéral considère que les systèmes de traitement de données automatisés exploités par les organes fédéraux dans le domaine de la coopération pénale instaurée par Schengen respectent les exigences de la norme européenne. Néanmoins, il n'est pas exclu que lors d'une future évaluation de la Suisse en matière de protection des données, les experts européens arrivent à une autre conclusion et recommandent à la Suisse de prendre les mesures techniques nécessaires pour que la journalisation du système de traitement automatisé examiné fournisse l'ensemble des informations prévues à l'art. 25 de la directive (UE) 2016/680. La mise en œuvre d'une telle recommandation entraînerait certaines conséquences financières qu'il n'est pas possible de chiffrer pour l'instant. Enfin, l'obligation pour les organes fédéraux d'annoncer leurs activités de traitement au préposé n'a pas de conséquence pratique, puisque cette obligation correspond en substance à l'obligation de déclarer un fichier prévu à l'art. 11*a*, al. 2, LPD.

Quant au registre des fichiers tenu par le préposé, il doit faire l'objet d'un remaniement puisque les fichiers des personnes privées n'y sont plus enregistrés, une fois la nouvelle loi entrée en vigueur, mais uniquement les activités de traitement des organes fédéraux.

11.4 Conséquences économiques

Le projet de loi vise un renforcement de la protection des données, au travers notamment d'une amélioration de la transparence des traitements et du contrôle des personnes concernées sur leurs données. Avec le développement des nouvelles technologies, il est en effet de plus en plus difficile pour celles-ci de savoir qui collecte des données à leur sujet, dans quel but et quels sont les destinataires de cette collecte. Le projet de loi vise également à renforcer la surveillance de l'application et du respect des dispositions fédérales de protection des données en octroyant des pouvoirs décisionnels au préposé, ce qui garantit une meilleure protection de la sphère privée des personnes concernées.

Le projet de loi vise en outre à faciliter les flux transfrontières en garantissant que les données peuvent transiter d'un pays à l'autre. En effet, la Suisse est considérée par les Etats membres de l'Union européenne comme un Etat tiers lorsque des données sont échangées dans le secteur privé. Aujourd'hui, la Suisse est au bénéfice d'une décision d'adéquation de la Commission européenne[314] selon laquelle le droit suisse offre un niveau de protection des données adéquat. En vertu de cette décision, une communication de données entre une entreprise privée établie sur le territoire d'un Etat membre et une personne privée située en Suisse est dès lors assimilée à une communication de données au sein de l'Union européenne. La décision de la Commission européenne peut toutefois être révisée en tout temps, comme le prévoit l'art. 46, par. 4 et 5, du règlement (UE) 2016/679. Le projet de loi a donc également pour objectif de permettre un rapprochement du droit fédéral avec les exigences européennes, de telle manière que la Suisse puisse conserver le cas échéant une décision d'adéquation de l'Union européenne. La ratification du protocole d'amendement de la convention STE 108 devrait permettre à la Suisse de continuer à garantir le flux transfrontière des données de et vers la Suisse à l'égard des pays de l'Union européenne d'une part – notons qu'il s'agira vraisemblablement d'une condition pour que l'Union européenne reconnaisse à la législation suisse un niveau de protection adéquat (art. 45 règlement [UE] 2016/679) – et à l'égard des pays non membres de l'Union européenne, mais ayant adhéré à la convention.

En élevant le niveau de protection des données aux standards européens, le projet de loi a également pour effet de renforcer la confiance des consommateurs envers le traitement de leurs données personnelles, notamment lors de transactions effectuées par voie électronique. De ce point de vue, le projet de loi peut engendrer des retombées positives non seulement pour les consommateurs, mais aussi pour les entreprises qui resteront attractives, et qui pourront développer de nouvelles opportunités d'affaires, particulièrement dans le domaine du commerce électronique. Les coûts nécessaires au respect des nouvelles obligations introduites par le projet de loi pour les responsables du traitement devraient ainsi être compensés, notamment par les avantages découlant du libre transfert des données avec l'Union européenne.

Par ailleurs il convient de relever que les entreprises suisses qui offrent des services dans les Etats membres doivent tenir compte du règlement (UE) 2016/679, vu son champ d'application territorial très large. Pour ces entreprises, le projet de loi n'implique pas de coûts supplémentaires trop élevés, puisqu'il contient des mesures similaires au règlement européen.

L'intervention de l'Etat est limitée au strict nécessaire, l'idée étant de responsabiliser les responsables du traitement en les encourageant à se soumettre à des codes de conduite ou encore à recourir à l'instrument de la certification. Une grande autonomie est également laissée aux acteurs économiques, qui peuvent s'assurer de l'existence d'un niveau de protection approprié des données lors de flux transfrontières par des mesures volontaires telles que l'élaboration de clauses types de protection des données personnelles ou de règles d'entreprise contraignantes et préalablement approuvées par le préposé. Les allégements apportés après la consultation externe, notamment en matière d'annonce, devraient limiter les charges administratives.

314 JO L 215 du 25.8.2000, p. 1.

11.5 Conséquences sociales et sanitaires

Pour répondre aux défis sociétaux que représentent les nouvelles technologies, le projet de loi prévoit notamment de renforcer les pouvoirs de surveillance du préposé. Il prévoit également d'attribuer à celui-ci la tâche de sensibiliser le public, et en particulier les personnes vulnérables telles que les personnes mineures ou les personnes âgées, à la protection des données.

Le renforcement de la législation améliore aussi la position des consommateurs, ainsi que celle des personnes vulnérables.

Aucune conséquence sanitaire directe n'est à signaler, sous réserve que le renforcement de la protection des données vaut également pour les traitements de données à des fins médicales.

11.6 Conséquences sur l'égalité entre hommes et femmes

Aucune conséquence sur l'égalité entre hommes et femme n'est à signaler.

11.7 Conséquences environnementales

Aucune conséquence directe sur l'environnement n'est à signaler.

12 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

12.1 Relation avec le programme de législature

Le projet a été annoncé dans le message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[315].

12.2 Relation avec les stratégies nationales du Conseil fédéral

Le projet est compatible avec la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), ainsi qu'avec la Stratégie *Open Government Data* (OGD). Par ailleurs le projet de loi fait partie du catalogue des mesures adopté pour la mise en œuvre de la Stratégie «Suisse numérique» (voir ci-dessus ch. 1.1.3).

315 FF **2016** 981, 1097

13 Aspects juridiques

13.1 Constitutionnalité

13.1.1 Compétence d'approbation de l'échange de notes concernant la reprise de la directive (UE) 2016/680

Selon l'art. 54, al. 1, Cst., les affaires étrangères relèvent de la compétence de la Confédération, le corollaire de cette compétence étant la conclusion de traités avec les Etats étrangers. En vertu de l'art. 166, al. 2, Cst., l'Assemblée fédérale est en principe compétente pour l'approbation des traités. Le Conseil fédéral ne peut lui-même conclure des traités internationaux que si une loi ou un traité international approuvé par l'Assemblée fédérale l'y autorise, ou s'il s'agit d'un traité de portée mineure (art. 166, al. 2, Cst., 24, al. 2, LParl et 7*a* LOGA).

Dans le cas présent, le Conseil fédéral ne dispose d'aucune compétence conférée par la loi ou un traité, car l'art. 36, al. 5, LPD ne s'applique pas. Par ailleurs, l'échange de notes concernant la reprise de la directive (UE) 2016/680 n'est pas de portée mineure. Il appartient donc à l'Assemblée fédérale de se prononcer sur l'approbation de cet échange de notes.

Conformément à l'art. 141, al. 1, let. d, Cst., les traités internationaux sont sujets à référendum lorsqu'ils sont d'une durée indéterminée et ne sont pas dénonçables (ch. 1), prévoient l'adhésion à une organisation internationale (ch. 2), ou contiennent des dispositions importantes fixant des règles de droit ou dont la mise en œuvre exige l'adoption de lois fédérales (ch. 3).

L'échange de notes entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 ne tombe pas sous le coup de l'art. 141, al. 1, let. d, ch. 1 et 2, Cst. Il demeure donc à examiner si cet accord contient des dispositions importantes fixant des règles de droit ou si leur mise en œuvre exige l'adoption de lois fédérales. Par «dispositions fixant des règles de droit», il faut entendre, selon l'art. 22, al. 4, LParl, les dispositions générales et abstraites d'application directe qui créent des obligations, confèrent des droits ou attribuent des compétences. Sont, par ailleurs, importantes les dispositions qui, en droit interne, doivent, à la lumière de l'art. 164, al. 1, Cst., être édictées sous la forme d'une loi au sens formel.

La mise en œuvre de l'échange de notes concernant la reprise de la directive (UE) 2016/680 implique plusieurs modifications législatives. Il résulte de ce qui précède que l'arrêté fédéral d'approbation de l'échange de notes entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680 est sujet au référendum en matière de traités internationaux en vertu de l'art. 141, al. 1, let. d, ch. 3, Cst.

13.1.2 Compétence d'approbation du protocole d'amendement de la convention STE 108

L'art. 4 du projet de protocole d'amendement de la convention STE 108 règle l'engagement des Etats parties. En vertu du par. 1, chaque Etat partie doit prendre, dans son droit interne, les mesures nécessaires pour donner effet aux dispositions de la future convention STE 108. Le par. 2 prescrit en outre que ces mesures doivent

entrer en vigueur au moment de la ratification ou de l'adhésion à la future convention STE 108. Selon l'art. 25 du projet, les Etats parties ne peuvent pas formuler des réserves.

Le projet de loi est conforme au P-STE 108. Dès que le protocole d'amendement de la convention STE 108 sera ouvert à la signature, le Conseil fédéral pourra le signer et proposer au Parlement de l'approuver. L'arrêté fédéral concernant l'approbation par la Suisse du protocole d'amendement de la convention STE 108 est sujet au référendum en matière de traités internationaux en vertu de l'art. 141, al. 1, let. d, ch. 3, Cst. pour les mêmes motifs que ceux exposés sous ch. 13.1.1.

13.1.3 Compétence législative de la Confédération

Ainsi que le relevait le Conseil fédéral dans son message du 19 février 2003 relatif à la révision de la LPD et à l'arrêté fédéral concernant l'adhésion de la Suisse au protocole additionnel à la convention STE 108[316], la Constitution ne contient aucune disposition habilitant expressément la Confédération à légiférer. L'art. 13, al. 2, Cst. consacre, par contre, le droit de toute personne d'être protégée contre l'emploi abusif de données la concernant. Il s'agit là d'un droit fondamental qui n'attribue pas de compétence nouvelle à la Confédération. En vertu de l'art. 35, al. 2 et 3, Cst., les personnes qui assument des tâches de l'Etat sont tenues de contribuer à la réalisation des droits fondamentaux et les autorités doivent veiller à ce que les droits fondamentaux, dans la mesure où ils s'y prêtent, soient aussi réalisés dans les relations qui lient les particuliers entre eux. Dans ce sens, le projet contribue à la réalisation de l'art. 13, al. 2, Cst., tant dans les relations verticales entre autorités et particuliers que dans les relations horizontales entre les personnes privées. Le P-LPD concrétise désormais les garanties de l'art. 13, al. 2, Cst. pour les personnes physiques. Pour les personnes morales, le Conseil fédéral propose d'insérer des règles minimales sur le traitement de données par des organes fédéraux dans la LOGA.

Par rapport à l'adoption de dispositions de protection des données applicables au domaine du droit privé, le législateur peut s'appuyer sur la compétence de légiférer en matière de droit civil (art. 122 Cst.), de même que sur la compétence de légiférer sur l'exercice des activités économiques lucratives privées (art. 95 Cst.) et sur la protection des consommateurs (art. 97, al. 1, Cst.).

Dans le domaine du droit public, le législateur fédéral s'est appuyé sur le pouvoir d'organisation que lui confère l'art. 173, al. 2, Cst. pour édicter des dispositions de protection des données applicables aux autorités et aux services administratifs.

La Constitution reconnaît aux cantons une pleine autonomie en matière d'organisation, de sorte qu'il leur appartient de légiférer sur la protection des données dans leur secteur. La Confédération n'est dès lors en droit d'édicter des dispositions de protection des données applicables aux secteurs publics cantonaux ou communaux que dans les domaines où les cantons sont chargés d'exécuter le droit fédéral, lequel doit être, il va sans dire, fondé sur une norme constitutionnelle attributive de compétence. Même dans ce cas, la Confédération doit toutefois éviter d'empiéter sur les

316 FF **2003** 1915, 1961

compétences cantonales en matière d'organisation. Le projet respecte cette limite. Les domaines dans lesquels il étend la protection des données concernent soit le traitement de données par des organes cantonaux en exécution du droit fédéral, soit le traitement de données par un organe fédéral conjointement avec des organes cantonaux. Enfin, le projet de loi abroge l'art. 37 LPD (exécution par les cantons).

13.2 Compatibilité avec les obligations internationales de la Suisse

Le projet de loi est compatible avec les obligations internationales de la Suisse (voir en particulier les ch. 1.2, 1.3, 2, 3, 4 et 9.3. Il permet à celle-ci de ratifier le protocole d'amendement de la convention STE 108 dès qu'il sera possible de le faire (cf. ch. 3.2 et 3.3). Il permet également à notre pays de respecter l'engagement pris dans le cadre de l'accord d'association à Schengen conclu avec l'Union européenne (cf. ch. 1.2.2.3, 2.2, 2.4 et 9.3).

L'art. 61 de la directive (UE) 2016/680 prescrit que les accords internationaux impliquant le transfert de données à caractère personnel à des pays tiers ou à des organisations internationales conclus par les Etats Schengen avant l'entrée en vigueur de la directive (UE) 2016/680 et qui respectent les dispositions pertinentes du droit de l'Union européenne applicables avant cette date, restent en vigueur jusqu'à ce qu'ils soient modifiés, remplacés ou révoqués[317].

Le projet de loi n'a pas non plus d'incidence sur la déclaration commune de la Suisse et de l'Union européenne sur l'art. 23, par. 7, de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne[318]. En effet, l'art. 60 de la directive (UE) 2016/680 prévoit que les dispositions particulières des actes juridiques de l'Union européenne adoptés avant l'adoption de la directive (UE) 2016/680, qui réglementent le traitement entre Etats membres, demeurent inchangées.

13.3 Forme de l'acte à adopter

La proposition comprend deux projets d'actes:

- Un projet d'arrêté fédéral portant approbation de l'échange de notes entre la Suisse et l'Union européenne concernant la reprise de la directive (UE) 2016/680.
- Un projet d'acte modificateur unique qui comprend le projet de loi fédérale sur la révision totale de la LPD et les adaptations nécessaires d'autres lois fédérales (ch. I et annexe) ainsi que les modifications des lois fédérales mettant en œuvre la directive (UE) 2016/680 dans le cadre des engagements Schengen (ch. II).

317 Consid. 95.
318 RS **0.362.31**

13.4 Frein aux dépenses

Le projet de loi n'implique pas de dépenses qui seraient assujetties au frein aux dépenses (art. 159, al. 3, let. b, Cst.).

13.5 Conformité à la loi sur les subventions

Le projet de loi ne prévoit pas de subventions.

13.6 Délégation de compétences législatives

Le P-LPD délègue des compétences législatives au Conseil fédéral dans les dispositions suivantes:

- Art. 11, al. 5 et 23, al. 6: le Conseil fédéral peut prévoir des exceptions aux obligations de tenir un registre des activités de traitement, ainsi qu'au principe de gratuité de droit d'accès.
- Art. 13, al. 3: le Conseil fédéral peut prévoit d'autres garanties appropriées pour communiquer des données personnelles à l'étranger.
- Art. 29: Lorsque l'organe fédéral traite des données personnelles conjointement avec d'autres organes fédéraux, avec des organes cantonaux ou avec des personnes privées, le Conseil fédéral règle les procédures de contrôle et les responsabilités en matière de protection des données.
- Art. 31: le Conseil fédéral conserve sa faculté d'autoriser, à certaines conditions, le traitement automatisé de données sensibles dans le cadre de projets pilotes.
- Art. 53: le Conseil fédéral peut déterminer dans quels cas il est possible de renoncer à percevoir un émolument ou le réduire.

13.7 Coordination avec d'autres lois fédérales

Lors des travaux parlementaires, il conviendra de modifier les lois fédérales suivantes qui sont entrées en vigueur après l'adoption du présent message:

- Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure: Les nouveaux art. 23*b* et 23*c* entrent en vigueur en même temps que la loi fédérale du 25 septembre 2015 sur le renseignement[319]. Il s'agira de remplacer à l'art. 23*b*, al. 2, let. c, la notion de «profil de la personnalité» par celle de «données personnelles» et de supprimer cette même notion à la phrase introductive de l'art. 23*c*, al. 2.

319 FF **2015** 6597

– Loi du 12 juin 2009 sur la TVA[320]: L'AFC traite et analyse de manière automatisée des données de personnes physiques (par ex., poursuites, acte de défaut de biens, erreurs de décompte, informations douanières, etc.) afin d'établir des profils de risque permettant de mieux cibler les contrôles fiscaux. L'AFC doit donc disposer d'une base légale au sens formel pour effectuer cette activité. Il faut supprimer le terme «profil de la personnalité» aux art. 76, al. 1, et 76*a*, al. 1, et habiliter l'AFC à effectuer des profilages. Il faut abroger l'art. 76*a*, al. 3, let. g. Il faut modifier l'art. 76*b*, al. 2, afin de permettre à l'AFC de communiquer des données, y compris à l'issue d'un profilage. Enfin, il faut ajouter à l'art. 76 un al. 1bis précisant que la personne mandatée est autorisée à accéder au système de traitement de l'AFC pour exercer son activité de surveillance.

– Loi fédérale du 25 septembre 2015 sur le renseignement: A l'art. 44, al. 1, la notion de «profil de la personnalité» doit être remplacée par l'expression «d'autres données personnelles permettant d'évaluer la menace qu'une personne représente». A l'art. 46, al. 1, la notion de «fichier» doit être remplacée par celle de «banque de données». A l'art. 61, al. 2, le renvoi à l'art. 6, al. 2, LPD doit être remplacé par un renvoi à l'art. 13, al. 1, P-LPD. L'art. 64 doit également être modifié sur différents points: l'al. 2 doit être adapté puisqu'en vertu de la future LPD le préposé ne rend plus de recommandations mais est habilité à ouvrir une enquête; l'al. 3 peut être abrogé l'intervention du Tribunal administratif fédéral n'étant plus nécessaire; l'al. 4 doit être modifié en ce sens qu'en cas d'erreur relative au traitement des données ou au report de la réponse, le préposé doit adresser au Service de renseignement de la Confédération (SRC) une décision lui ordonnant d'y remédier; l'al. 5 doit être modifié en ce sens que le préposé peut ordonner au SRC de fournir à la personne concernée les renseignements demandés si les conditions prévues par cette disposition sont remplies. En ce qui concerne l'art. 65, il peut être supprimé pour les mêmes motifs que ceux indiqués pour l'art. 64, al. 3; il y a également lieu de supprimer le renvoi à l'art. 65, al. 1, contenu à l'art. 66, al. 1. Enfin, la terminologie de l'art. 78 doit également être adaptée: la notion de maître du fichier doit être remplacée par celle de «responsable du traitement»; quant à la notion de «fichier», elle doit être remplacée par celle de «système d'information, banque de données et dossiers papier».

– Loi du 20 juin 2014 sur la nationalité suisse[321]: Cette loi entre en vigueur le 1er janvier 2018. Il y a lieu de prévoir une modification de l'art. 44: la notion de «profil de la personnalité» doit être remplacée par l'expression «des données permettant d'évaluer l'aptitude du requérant à la naturalisation».

– Loi du 3 février 1995 sur l'armée: Le nouvel art. 100 entre en vigueur le 1er janvier 2018[322]. Il y a lieu de remplacer, à l'al. 3, let. a, la notion de «profil de la personnalité» par celle de «données personnelles permettant d'évaluer la menace qu'une personne représente» et de renvoyer, à la let. b, aux

320 RS **641.20**, modification du 30 septembre 2016, RO **2017** 3575
321 FF **2014** 5001
322 FF **2014** 6803

art. 13 et 14 P-LPD. A l'al. 4, let. c, ch. 2, la notion de «fichier» est remplacée par celle d'«activité de traitement».

Lors des travaux parlementaires, il conviendra également de formuler des normes de coordination entre le projet de loi et les lois fédérales suivantes, dont la date d'entrée en vigueur n'est pas encore connue:

- Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication[323]: A l'art. 4, il s'agit de supprimer la notion de «profil de la personnalité». A l'art. 13, la notion de «maître du fichier» doit être remplacée par celle de «responsable du traitement».
- Modification du 18 mars 2016 de la loi sur les produits thérapeutiques[324]: A l'art. 62*a*, il s'agit de supprimer la notion de «profil de la personnalité».
- Loi fédérale du 17 juin 2016 sur le casier judiciaire[325]: Il s'agit de remplacer à l'art. 3, al. 1, la notion de «maître du fichier» par celle de «responsable du traitement». A l'art. 12, al. 2, le terme «fichier» peut être remplacé par «banque de données». Enfin, la notion «fichier journal» peut être supprimée à l'art. 25, al. 1.
- Loi fédérale du 30 septembre 2016 sur l'énergie[326]: Du fait de la suppression, dans le P-LPD, de la protection des données concernant des personnes morales et de la limitation, à l'art. 4, let. a, P-LPD, de la définition des données personnelles aux informations concernant une personne physique identifiée ou identifiable, il faut modifier la terminologie des art. 56, al. 1, 58, titre et al. 1 et 3, et 59, titre et al. 1 et 2, afin d'établir clairement que ces dispositions s'appliquent également aux données concernant des personnes morales. Il faut remplacer l'expression «données personnelles» par «données personnelles et données concernant des personnes morales». Il faut par ailleurs, et pour les mêmes raisons, effectuer les modifications suivantes dans la loi du 23 mars 2007 sur l'approvisionnement en électricité[327], que doit modifier la loi du 30 septembre 2016 sur l'énergie: l'art. 17*c*, al. 1, doit être complété en ce sens que la LPD s'applique par analogie au traitement de données concernant des personnes morales. A l'art. 27, al. 1, l'expression «données personnelles» doit être remplacée par «données personnelles et données concernant des personnes morales».
- Modification du 16 juin 2017 de la loi sur le personnel de la Confédération[328]: Il s'agit de supprimer à l'art. 27, al. 2, la notion de «profils de la personnalité».
- Modification du 16 juin 2017 de la loi sur l'aviation[329]: Il s'agit de supprimer à l'art. 21*c*, al. 1, let. b, la notion de «profil de la personnalité».

323 FF **2016** 1821
324 FF **2016** 1781
325 FF **2016** 4703
326 FF **2016** 7469
327 RS **734.7**; cf. FF **2016** 7469, 7514 ss
328 RS **172.220.1**; cf. FF **2016** 271, 323
329 FF **2017** 3993

– Loi sur l'enregistrement des maladies oncologiques du 18 mars 2016[330]: La notion de «maître du fichier» est remplacée, à l'al. 7, al. 2, par celle de «responsable du traitement».

13.8 Coordination avec d'autres projets législatifs

Le projet de loi pourra avoir une influence sur les actes suivants en cours de révision:

– Projet de loi fédérale sur les jeux d'argent[331]: Il s'agira de modifier les bases légales relatives aux profils de la personnalité.

– Projet de loi sur l'analyse génétique humaine (LAGH).

– Projet de loi sur l'organisation de l'infrastructure ferroviaire[332].

– Projet de révision de la loi fédérale sur les télécommunications[333]: Le message du Conseil fédéral devrait être adopté à la fin de l'été 2017. Il s'agira le cas échéant d'adapter certains termes de protection des données à la nouvelle terminologie de la future LPD.

– Projet de révision de la loi sur les étrangers: Le message du Conseil fédéral devrait être adopté durant l'automne 2017. Il s'agira le cas échéant d'adapter certains termes de protection des données à la nouvelle terminologie de la future LPD.

– Projet de modification du code civil (Enregistrement de l'état civil et registre foncier)[334]: Il s'agira de tenir compte de la nouvelle teneur de l'art. 45*a* CC et de l'adapter si nécessaire.

– Avant-projet de loi fédérale sur le traitement des données personnelles par le Département fédéral des affaires étrangères: Il s'agira le cas échéant d'adapter la terminologie de cet acte et de supprimer la notion de «profil de la personnalité».

– Projet de modification de la loi sur la surveillance des marchés financiers (dans le cadre du projet de loi sur les établissements financiers)[335]: A l'art. 13*a*, al. 2, il faudra supprimer l'expression «profils de la personnalité». A l'art. 13*a*, al. 1, il faudra préciser que la FINMA peut traiter, outre les données concernant ses employés, celles de «candidats à un poste». A la liste des tâches pour lesquelles la FINMA traite des données, il faudra ajouter «les procédures de recrutement». Enfin, il faudra préciser que la FINMA peut confier le traitement de données à des agents spécialisés.

330 FF **2016** 1767
331 FF **2016** 7769
332 FF **2016** 8487
333 RS **784.10**
334 FF **2014** 3429
335 FF **2015** 8335