Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik

21 décembre 2016

Rapport explicatif concernant l'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

Table des matières

Condensé

La présente révision 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. La révision 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. Elle vise de plus à renforcer la surveillance de l'application et du respect des dispositions fédérales de protection des données. Enfin, elle 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 de la révision
La présente révision a pour origine une décision du Conseil fédéral de préparer un avant-projet de loi qui doit poursuivre principalement deux objectifs : la révision doit d'une part renforcer les dispositions légales de protection des données pour faire face au développement fulgurant des nouvelles technologies et d'autre part tenir compte des réformes du Conseil de l'Europe et de l'Union européenne en la matière. Ce projet figure parmi les objectifs du Conseil fédéral de 2016 et dans le programme de législature 2015-2019. 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.

Les développements internationaux témoignent également de l'importance toujours plus grande accordée à la protection des données personnelles. Ainsi, 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 devrait être adopté début 2017.

La révision 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. Elle 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 de 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 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 des conditions déterminantes pour que la Commission européenne maintienne la décision d'adéquation accordée à la Suisse selon laquelle cette dernière offre un niveau de protection des données adéquat. Cette décision a une importance centrale surtout pour l'économie suisse.

Contenu du projet de révision
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 d'information lors de décisions individuelles automatisées ainsi que le droit pour la personne concernée de faire

valoir son point de vue dans ce cas. 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'auto-réglementation, notamment par le biais de recommandations de bonnes pratiques qui visent à faciliter les activités des responsables du traitement et à contribuer au respect de la législation. Ces recommandations sont adoptées par le Préposé fédéral à la protection des données et à la transparence qui doit associer les milieux intéressés. Ces derniers peuvent également édicter leurs propres recommandations et les faire approuver.

Le statut et l'indépendance du Préposé fédéral à la protection des données et à la transparence 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 demande.

Le volet pénal de la législation fédérale sur la protection des données est renforcé à plusieurs égards, pour compenser notamment le fait que le Préposé fédéral à la protection des données et à la transparence, contrairement à la quasi-totalité de ses homologues européens, n'a pas le pouvoir d'infliger des sanctions administratives.

Enfin, en sus de la révision de la loi fédérale sur la protection des données, certaines lois fédérales doivent être révisées. Il s'agit en particulier de transposer certaines exigences de la directive (UE) 2016/680 dans le code pénal, le code de procédure pénale, la loi sur l'entraide pénale internationale et d'abroger certaines dispositions de la loi sur l'échange d'information Schengen.

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 régit 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 toute collecte de données personnelles ne peut être entreprise que d'une manière licite (art. 4, al. 1), que le traitement de ces dernières doit être effectué conformément aux principes de la bonne foi et de la proportionnalité (art. 4, al. 2) et uniquement dans le but qui est indiqué lors de la collecte, qui est prévu par une loi ou qui ressort des circonstances (art. 4, al. 3). La collecte de données, 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 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. 10a régit le traitement de données par un tiers. L'art. 11a prévoit une obligation pour le Préposé fédéral à la protection des donnée et à la transparence (ci-après « 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, 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 personnalité les concernant, sous réserve d'exceptions. La LPD 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. 18a 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. 18b). 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

[1] RS **235.1**

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 26a 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 (et 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. L'efficacité de LPD doit pour cette raison être améliorée. En effet, cette loi ne suffit plus dans certains contextes à garantir une protection suffisante. Se fondant sur les conclusions du 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 Dépar-

---

2 BÜRO VATTER/INSTITUT FÜR EUROPARECHT, Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht, Bern 11 März 2011. https://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 : 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 https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf.

tement fédéral de l'intérieur (DFI), un avant-projet de loi, en tenant compte des conclusions dudit rapport et des réformes du Conseil de l'Europe et de l'Union européenne.

Le Conseil fédéral a décidé de mettre en consultation un avant-projet d'acte modificateur unique sujet au référendum (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 ; ci-après « AP »). Le chiffre I de l'acte modificateur unique comprend la révision totale de la LPD (ci-après « AP-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 à Schengen. Les actes législatifs modifiés sont désignés dans le présent rapport, par « AP », suivi de l'abréviation de la loi concernée (voir ch. 8.2 et 8.3).

1.1.3 Stratégie Suisse numérique

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

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 publique 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 données. 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[9], qui comprend les mesures que l'administration fédérale doit mettre en œuvre, a été mis en place. L'AP fait partie d'une de ces mesures (ch. 1.2 et 1.7 du plan d'action).

Dans le cadre de l'élaboration de cette stratégie, l'OFCOM a fait réaliser une étude sur la problématique du Big Data par la Haute école bernoise, intitulée « Big Data: atouts, risques et mesures nécessaires pour la Confédération »[10]. 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 l'AP 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 touchent la protection des données. Parmi les projets en cours, on peut citer les suivants, qui sont les plus importants :

Stratégie nationale de protection de la Suisse contre les cyberrisques du 27 juin 2012 (SNPC)[11] *:* 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.

---

9 https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/strategie-suisse-numerique/plan-daction.html.

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

11 https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html.

Stratégie Open Government Data du 16 avril 2014 (OGD) [12]: 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)[13] : 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 du « Big Data », et un module sur le développement d'applications des mégadonnées dans différents domaines de la société.

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 (par ex. le droit civil, 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 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 »[14] mis en œuvre de 2011 à 2015. Le DFI (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 sur les conditions-cadres pour une économie numérique : le rapport traite de différents domaines qui ont une importance déterminante pour l'économie numérique. Cinq domaines sont visés : le marché du travail, la recherche et le développement, l'économie de partage, la finance numérique et la politique de la concurrence. Le rapport examinera ces domaines. Le cas échéant, il proposera des adaptations de la réglementation pour créer, avec des conditions-cadres attractives de politique économique, un environnement positif à l'économie numérique.

1.1.5 Interventions parlementaires

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

- Initiative parlementaire Vischer 14.413 « Droit fondamental à l'autodéterrmination en matière d'information ». Selon son auteur, l'art. 13 al. 2 Cst. 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.

[12] https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn004-open_government_data_strategie_schweiz.html.

[13] http://www.nfp75.ch/fr.

[14] http://www.jeunesetmedias.ch/fr/accueil.html

- 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. Celle-ci 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[15].
- 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 également été partiellement réalisé par le rapport du Conseil fédéral du 9 décembre 2011[16].
- 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 », qui demande la création d'une commission d'experts interdisciplinaire pour assurer au mieux à l'avenir le 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 de la révision de la LPD (voir ch. 1.1.4); toutefois, certaines mesures allant dans le sens de la réalisation de la motion peuvent être réalisées dans le cadre de cette révision.
- Postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication » : le Conseil national 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.

[15] FF **2012** 255, 270

[16] FF **2012** 255, 270

- 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 29 octobre 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 »: cette intervention a été adoptée par le Conseil national le 20 mars 2015. Celle-ci a la même teneur que celle du Postulat Comte 14.4284 « Enregistrements vidéo par des privés. Mieux protéger la sphère privée ».
- Postulat Comte 14.4284 « Enregistrements vidéo par des privés. Mieux protéger la sphère privée » : cette intervention a été adoptée par le Conseil aux Etats le 19 mars 2015. L'auteur demande au gouvernement 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.
- Postulat Derder 15.4045 «Droit d'exploiter des données personnelles. Droit d'obtenir une copie» : le Conseil national adopté cette intervention le 18 décembre 2015. Celle-ci 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.
- Motion Béglé 16.3379 « Promouvoir la Suisse en tant que coffre numérique universel ». Cette motion charge le Conseil fédéral de maintenir dans le cadre de la révision la protection des données des personnes morales (ch. 1) ainsi que l'art. 11 LPD qui prévoit une certification facultative (ch. 2). L'auteur de la motion estime que ces dispositions sont importantes pour assurer un niveau de protection des données optimal et de positionner ainsi la Suisse comme coffre-fort numérique universel. Cette motion a été traitée au Conseil national le 30 septembre 2016. Le ch. 1 a été rejeté, et le ch. 2 adopté.
- 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 (LPD) ». 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 « 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. Dans sa réponse, le Conseil fédéral propose l'adoption et précise, qu'indépendamment de la révision

en cours, la thématique de la réappropriation des données personnelles sera examinée en lien avec la stratégie « Suisse numérique ».

1.2 Contexte international

1.2.1 Remarque préliminaire

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 sur 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 (art. 8 de la Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales[17], art. 17 du Pacte international du 16 décembre 1966 relatif aux droits civils et politiques[18]), d'autres droits peuvent être touchés: les libertés d'opinion et d'information (art. 16 Cst., art. 10 CEDH, art. 19 du Pacte II de l'ONU), la liberté de réunion (art. 22 Cst., art. 11 CEDH, art. 21 du Pacte II de l'ONU), la liberté d'association (art. 23 et 28 Cst., art. 11 CEDH, art. 22 du Pacte II de l'ONU) et le droit à la famille (art. 14 Cst., art. 8 et 12 CEDH, art. 23 du Pacte II de l'ONU).

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[19]. 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, 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 (par ex. habitudes alimentaires, état de santé, etc.).

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[20] 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[21] 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 »).

---

17 CEDH, RS **0.101**

18 Pacte ONU-II, RS **0.103.2**

19 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.

20 JO L 281 du 23.11.1995, p. 31.

21 JO L 350 du 30.12.2008, p. 60.

Dans le cadre du programme de Stockholm[22], 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 des 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 »[23], 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[24] relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (ci-après « 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[25] 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 (ci-après « 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 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)[26]. 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.

1.2.2.2 Décision d'adéquation

Dans les domaines qui ne relèvent pas de la coopération instaurée par Schengen, 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[27]. Cette décision se fonde toutefois sur le niveau de protection défini par la directive 95/46/CE. 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, il est essentiel que sa législation corresponde aux exigences du règlement (UE) 2016/679.

---

22 JO C 115, du 4.5.2010, p. 1.

23 COM (2010) 609 final.

24 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.

25 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.

26 RS **0.362.31**

27 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

1.2.2.3 Recommandations suite à l'évaluation Schengen

En s'associant à Schengen, 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.

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. 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.

L'AP-LPD donne suite aux recommandations du Conseil, dans la mesure où des compétences décisionnelles sont conférées au préposé (voir art. 41 à 43 AP-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

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 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après « convention STE 108 »)[28] 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[29] (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 (voir 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 dans l'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 (ci-après « P-STE 108 »). Les travaux du Comité ad hoc établi par le Comité des Ministres se sont terminés en juin 2016. Le protocole d'amendement de la convention STE 108 devrait être adopté par le Comité des Ministres début 2017 (voir ci-après ch. 3.2). Le présent rapport se base sur le projet de modernisation en l'état en septembre[30], 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 euro-

---

[28] RS **0.235.1**

[29] RS **0.235.11**

[30] Le texte français peut être consulté à l'adresse suivante : http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Version%20consolidée%20convention%20108%20modernisée%20juillet%202016.pdf . Une traduction allemande et une traduction italienne sont jointes au dossier pour la consultation externe.

péenne, 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[31]. Cette dernière 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[32]. 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 et participé activement à ces deux initiatives.

Le rapporteur spécial a rendu son premier rapport le 8 mars 2016. Il estime 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. Un point notamment qui reste à clarifier concerne le risque de violation du droit à la sphère privée par une utilisation abusive des données personnelles par des entreprises privées[33]. Globalement, les craintes quant à une utilisation abusive des données se sont reportées des Etats sur les entreprises[34]. Le rapporteur spécial estime ainsi 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. Dans ce but, il prévoit de mener d'ici à 2017, dans le cadre du projet « Corporate online business models and personal data use », une vaste consultation auprès des entreprises et de la société civile[35].

Le rapporteur spécial observe en outre une prise de conscience des consommateurs sur les risques qui pèsent sur leur sphère privée ; en témoigne par exemple le développement rapide d'un marché des produits et services respecteux de la sphère privée[36]. Il s'oppose au développement de législations nationales obligeant les entreprises à intégrer dans leurs produits des « portes dérobées » qui permettraient d'accéder ultérieurement à des données cryptées[37]. 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 et que sur le plan légal[38].

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[39] – élaborées en 1980 et révisées en 2013 –

---

31 Résolution 68/167 du 18 décembre 2013 disponible en français au lien suivant : http://www.un.org/fr/documents/view_doc.asp?symbol=A/RES/68/167

32 HCDH « Le droit à la vie privée à l'ère du numérique », 2014.

33 HRC, Special Rapporteur Right to Privacy 2016, ch. 9.

34 HRC, Special Rapporteur Right to Privacy 2016, ch. 9.

35 HRC, Special Rapporteur Right to Privacy 2016, ch. 9 et ch. 46s.

36 HRC, Special Rapporteur Right to Privacy 2016, ch. 50.

37 HRC, Special Rapporteur Right to Privacy 2016, ch. 30 s.

38 HRC, Special Rapporteur Right to Privacy 2016, ch. 15 et 46e.

39 Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 1980, consultables à l'adresse: http://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 : https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

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 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)[40]. 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[41]. 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[42]. 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 ou que des garanties suffisantes existent que le niveau de protection exigé par les lignes directrices est respecté.

1.3 Objectifs de la révision

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. Ce projet figure également parmi les objectifs du Conseil fédéral de 2016 et dans le programme de législature 2015-2019 (ch. 10.1). Celui-ci réalise également une grande partie des interventions parlementaires figurant sous ch. 1.1.5.

L'AP poursuit plusieurs objectifs qui se complètent mutuellement.

Le projet 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.

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 per-

[40] OCDE, Lignes directrices régissant la protection de la vie privée 1980, principes 6 à 14 ; OECD, Privacy Framework 2013, pp. 22 et 47 s.

[41] OECD, Lignes directrices régissant la protection de la vie privée 2013, principes 16 à 18, 19 let. g et 20 à 23.

[42] OCDE, Lignes directrices sur la protection de la sphère privée, principe 16.

sonnelles 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 de 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 rapport explicatif. Il ne devrait ainsi pas y avoir de procédure de consultation externe ultérieure.

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 de l'AP-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, l'AP-LPD traite de manière égale les différentes technologies. La loi peut ainsi s'adapter aux évolutions technologiques sans freiner l'innovation. L'exigence de base légale formelle pour les « procédures d'appel » dans le secteur public est abandonnée, car elle va à l'encontre du caractère technologiquement neutre du projet.

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 européen. 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 identifiant un individu de manière unique ».

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 reste le même. Toutefois, il incombe désormais au Conseil fédéral, et non plus au responsable du traitement, de déterminer si la législation d'un Etat tiers remplit cette exigence. A défaut d'une telle législation, l'AP-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. L'AP-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 du traitement. 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 ses homologues européens, il n'est toutefois pas habilité à prononcer des sanctions administratives. Cette restriction est compensée par un net renforcement des dispositions pénales de la loi.

1.4.2 Principales nouveautés

1.4.2.1 Modification du champ d'application de la future LPD

L'AP-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.

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

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 (par ex. des décisions fondées uniquement sur des algorithmes, sans intervention humaine), ainsi que le droit pour la personne concernée de faire valoir son point de vue. L'AP étend également la liste des informations à fournir à la personne concernée lorsque celle-ci exerce son droit d'accès.

Les droits des personnes concernés sont clarifiés sur différents points. Entre autres, l'AP-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.

1.4.2.3 Encouragement de l'auto-réglementation

La révision encourage le développement de l'auto-réglementation et la responsabilisation des responsables du traitement. Afin de faciliter leurs tâches et d'assurer un meilleur respect

de la loi, le préposé a pour tâche d'édicter des recommandations de bonnes pratiques. Cette tâche n'est pas entièrement nouvelle puisque le préposé publie déjà des recommandations générales sur son site, mais elle devrait se développer à l'avenir. Le préposé doit associer les milieux intéressés, lesquels peuvent aussi édicter leurs propres recommandations et les faire approuver par le préposé.

Les recommandations de bonnes pratiques permettent d'avoir des règles plus précises dans des domaines qui suscitent aujourd'hui de nombreuses questions, de préciser certaines notions, les modalités de certains droits ou de certains devoirs, mais aussi de mieux responsabiliser les responsables du traitement.

Les recommandations de bonnes pratiques n'ont pas de caractère obligatoire, mais concrétisent les dispositions légales. En s'y conformant, le responsable du traitement respecte par là-même ces dernières.

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

Le statut et l'indépendance de l'institution du préposé sont renforcés. Ce dernier peut effectuer trois mandats au maximum et ne peut exercer une activité accessoire qu'à des conditions strictes. L'AP-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 demande. 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 la quasi-totalité de ses homologues européens, n'a pas le pouvoir d'infliger des sanctions administratives. Ce renforcement comprend : l'augmentation du seuil maximum des amendes à 500'000.- ; l'adaptation de la liste des comportements punissables aux nouvelles obligations des responsables du traitement et des sous-traitants; l'institution d'un délit passible de la peine privative de liberté concernant la violation du devoir de discrétion ou la prolongation du délai de prescription de l'action pénale pour les contraventions. En cas de contravention commise dans une entreprise, les autorités de poursuite pénale – en l'occurrence les cantons – peuvent à certaines conditions renoncer à poursuivre les personnes responsables et condamner l'entreprise au paiement de l'amende.

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, l'AP 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, l'AP 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.

Etant donné que la loi ne s'applique plus aux registres publics relatifs aux rapports de droit privé, il convient de modifier la législation fédérale sur l'état civil, notamment en ce qui concerne la surveillance du respect des exigences de protection des données et les droits des personnes concernées.

1.6 Autres mesures examinées

Dans le cadre des travaux de révision, le Conseil fédéral a examiné d'autres mesures mais il a finalement décidé de ne pas intégrer dans l'AP. Il s'agit principalement des suivantes :

1.6.1 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. Certes, cette solution a le mérite de permettre au préposé d'obliger directement les destinataires des règles en questions. Elle soulève toutefois bon nombre de problèmes en lien avec le principe de la légalité (délégation de compétence au préposé, densité normative). Par rapport à la solution retenue par l'AP concernant les recommandations de bonnes pratiques, le processus d'adoption serait plus lent, dans la mesure où l'on devrait suivre le processus législatif applicable aux ordonnances de l'administration fédérale. Par ailleurs, cette option laisse peu de marge de manœuvre aux milieux concernés ce qui peut nuire à l'acceptation de ces règles.

1.6.2 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 du 19 décembre 1986 contre la concurrence déloyale (LCD)[43]. 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.

1.6.3 Exercice collectif des droits

Il n'est pas prévu d'introduire un système d'exercice collectif des droits (extension du droit d'action des organisations et institution d'actions de groupe ou de transactions de groupes) qui soit limité à la protection des données. Ces instruments seront examinés, dans un contexte plus large, dans le cadre de la mise en œuvre de la motion 13.3931 Birrer-Heimo.

1.6.4 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'étude 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 prévoit 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 ».

1.6.5 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 les recommandations de bonnes pratiques, non pas au préposé, mais à une commission extra-parlementaire. La solution de préposé présente toutefois l'avantage de ne pas engendrer de charges administratives et financières supplémentaires et garantit une intervention rapide.

---

[43] RS **214**

1.6.6 Modification de l'organisation de l'autorité de contrôle

Il a été envisagé de modifier l'organisation du préposé et d'en faire 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, et dans de nombreux pays européens (Allemagne, Espagne, ou Pologne).

1.6.7 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 aurait entrainé des conflits de compétences. Par ailleurs, la création d'un organe rattaché au préposé entraîne des coûts importants qui sont été en contradiction avec la politique budgétaire actuelle du Gouvernement.

1.7 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)[44].

L'OFJ et le Secrétariat d'Etat à l'économie (SECO) ont mandaté l'entreprise PwC pour qu'elle procède à une AIR[45] qui puisse servir de base pour l'évaluation des effets de la révision. 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, le 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.

1.7.1 La nécessité et la 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 de nouvelles craintes au sein de la population et qui ont entraîné de nouvelles menaces pour la protection des données. A cet égard, l'AP vise 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.

1.7.2 L'impact du projet sur les différents groupes de la société

Les modifications envisagées par l'AP concernent toutes les entreprises actives en Suisse. Pour cette AIR, ces dernières ont été segmentées d'après leur «exposition au droit de la protection des données», matérialisée par branche et par taille. Les segments suivants ont été formés:

- Segment A: *entreprises faiblement exposées au droit sur la protection des données*

[44] RS **171.10**

[45] L'AIR est disponible sur le site Internet de l'office : https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

- 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 8'000 dans le segment C (1. 4%).

Les résultats de l'analyse montrent que les entreprises du segment A sont généralement peu touchées par les mesures prévues dans le cadre de l'AP. Ainsi, l'impact de la révision sur ce segment est relativement faible. 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 faudra 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[46].

1.7.3 Les implications pour l'économie dans son ensemble

Il convient de distinguer les effets de la révision 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 sont propres ou qui sont 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, la révision ne prévoit aucune obligation per se pour les personnes concernées. Elle prévoit au contraire le renforcement de leur position. 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 depuis renoncé pour le moment (ch. 1.6.4). La question de savoir si les personnes concernées profiteront concrètement des mesures examinées dépendra surtout de l'importance accordée par ces dernières 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.

1.7.4 Les 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, tel 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 a été saluée car elle permet de s'adapter rapidement aux nouveautés technologiques (ch. 1.6.5).

[46] Voir le tableau récapitulatif en page 54 à 58 de la AIR pour une vision détaillée des impacts pour chaque mesure.

1.7.5 Les aspects pratiques de l'exécution

Pour limiter les coûts liés à la révision, 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 le site Internet ou dans les 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, l'AP 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 du traitement. 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, guides) et le développement de recommandations de bonnes pratiques: 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 est dans ce contexte accueillie favorablement par la majorité des experts.

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 l'espace 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'Union européenne. 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 autorités 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 consulter le cas échéant l'autorité de contrôle (art. 28). Les art. 30 et 31 introduisent une obligation pour le responsable du traitement de notifier 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, 46 et 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 tels 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, al. 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 donc 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 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, 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 l'AP-LPD et s'appliquent à l'ensemble 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 l'AP-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 domaines soumis à la LPD. 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 (voir ch. 8.3).

Le tableau de concordance en annexe du présent rapport indique pour chaque disposition de l'AP-LPD les dispositions correspondantes du P-STE 108 et de la directive (UE) 2016/680.

2.4 Principales modifications législatives nécessaires

En sus des modifications à apporter à la LPD, les législations fédérales à réviser sont les suivantes: le code pénal suisse du 21 décembre 1937 (CP)[47], le code de procédure pénale du 5 octobre 2007 (CPP)[48], la loi fédérale du 20 mars 1981 sur l'entraide pénale internationale (EIMP)[49], la loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[50], la loi du 12 juin 2009 sur l'échange d'informations Schengen (LEIS)[51] et 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 (LOC)[52]. Les dispositions de la directive (UE) 2016/680 qui doivent être transposées dans l'AP-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.

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 de notifier 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 le principe de la protection des données dès la conception et par défaut (art. 8bis par. 2 et 3).

---

47 RS **311.0**

48 RS **312**

49 RS **351.1**

50 RS **351.93**

51 RS **362.2**

52 RS **360**

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. Les conditions applicables au consentement de la personne concernée doivent de plus être 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 transfert 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. 49 Etats ont ratifié le texte actuel, dont deux Etats qui ne sont pas membres du Conseil de l'Europe (Uruguay, Maurice) ; plusieurs autres Etats non membres du Conseil de l'Europe sont également en passe de la ratifier (Maroc, Tunisie, Sénégal). 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 à 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 signature du projet 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 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 en faveur d'un renforcement de la protection des données dans le cadre de son action en faveur des droits de l'homme[53]. Enfin, il convient de relever que les mesures prévues par le P-STE 108 convergent avec les

[53] 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 »).

objectifs annoncés par le Conseil fédéral dans sa décision du 9 décembre 2011 sur la base des résultats de l'évaluation de la LPD[54].

En ce qui concerne la procédure de ratification de la future convention STE 108, l'art. 4 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 de l'AP 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.

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 l'AP-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, celles-ci 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, de notifier 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).

[54] FF **2012** 255

Le chapitre V du règlement (UE) 2016/679 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. 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) 679/2016 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. 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. 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[55] constatant qu'elle garantit un niveau adéquat de protection des données. Cette décision peut néanmoins être révisée en tout temps. 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 sont à l'avenir déterminants pour juger du caractère adéquat de la protection offerte par la législation suisse. L'AP devrait permettre d'assurer un niveau de protection adéquat au sens du règlement.

[55] JO L 215 du 25.8.2000, p. 1.

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

Les pays européens ne sont pas les seuls à avoir adopté une législation sur la protection des données comme le montrent les quelques exemples ci-dessous[56].

5.1 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[57]. Elle a un rôle d'assistance, de conseil et de surveillance. L'art. 29 du Décret 1558/2001[58] lui permet également d'établir des règles administratives et de procédure par rapport au registre des bases de données personnelles (le Registre), 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).

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 et/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 registre, veiller à la sécurité des données stockées, garantir la confidentialité des données ainsi que fournir les documents et renseignements sollicités par la DNPDP.

La législation sur la protection des données s'applique aussi au Big Data 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.

---

[56] Ces informations se basent sur un avis de droit de l'ISDC du 3 août 2016.

[57] Ley 25.326, Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales. Sancionada: Octubre 4 de 2000, disponible sous http://www.jus.gob.ar/media/33481/ley_25326.pdf.

[58] Decreto 1558/2001, Protección de los datos personales, disponible sous http://www.jus.gob.ar/media/33382/Decreto_1558_2001.pdf.

5.2 Nouvelle-Zélande

En Nouvelle-Zélande, la protection des données est principalement régie par le «Pricacy Act 1993»[59]. 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» (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[60] 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 à la protection des données, et une nouvelle 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(1)(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.

5.3 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»[61] (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 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 durant 3 ans (art. 9 PIPA) ainsi que des lignes directrices (art. 12 PIPA).

---

[59] Le «Privacy Act 1993» est disponible ici: http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.

[60] Est considérée comme «agency» presque toutes les personnes et organisations qui détiennent des données personnelles.

[61] Les textes légaux sont disponibles en anglais ici: http://www.law.goper.kr/eng/engMain.do.

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). Ce dernier 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 rempli 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 l'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 à minimiser les risques de violations de la vie privée (art. 3 par. 6 PIPA) et de travailler en anonymisant 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.

5.4 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)[62]) 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 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 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 particu-

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

liers (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.

5.5 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)[63], 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 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 divulguées 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 divulguent 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

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

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.

6 Mise en œuvre

A l'occasion 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 recommandations de bonnes pratiques permettent d'introduire des règles plus précises, en tenant compte des caractéristiques des différents domaines.

Au demeurant, l'ordonnance sur la protection des données sera adaptée afin de ne pas surcharger la loi de détails.

Si l'AP 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 l'acceptation 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.

7 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 l'AP-LPD, le 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 recommandations de bonnes pratiques.
- 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. L'AP-LPD prévoit des mesures pour améliorer la protection de ces derniers.
- Postulats Groupe libéral-radical 14.4137 et Comte 14.4284 « Enregistrements vidéo par des privés. Mieux protéger la sphère privée ». L'AP-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 sanctionné

plus efficacement. Associée aux dispositions pénales actuelles sur les infractions contre le domaine secret ou le domaine privé, cette modification offre une protection élargie.

- 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 CP, de l'art. 179decies.
- Postulat Béglé 16.3383 « Données numériques : informer les personnes lésées en cas de piratage ». L'AP (art. 17) prévoit une notification des violations de la protection de données, au préposé, et, dans certaines situations, à 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 (LPD) ». La LPD s'applique aux données médicales dans la mesure où aucune loi spéciale ne prévoit le contraire. L'AP prévoit toute une série de nouvelles obligations à charge du responsable du traitement et du sous-traitant qui s'appliqueront donc aussi aux données médicale (art. 13, 15, 16, 17, 18 et 19) qui vont dans le sens du postulat. D'autres mesures, telles que la précision des exigences du consentement (art. 4, al. 6), ou encore l'élaboration de recommandations de bonnes pratiques, devraient aussi permettre d'améliorer la protection des données médicales.

Les interventions parlementaires suivantes sont classées partiellement :

- 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 de la révision. 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. Un examen plus poussé de la question de l'identité numérique pourrait se faire dans le cadre des travaux du groupe d'experts « Avenir du traitement et de la sécurité des données » ou dans le cadre de la « Stratégie Suisse numérique ».
- Postulat Schwaab 14.3739 « Control by design. Renforcer les droits de propriété pour empêcher les connexions indésirables ». L'AP-LPD réalise le postulat partiellement en ce sens que son contenu protège mieux à l'avenir les personnes concernées. L'objet de ce postulat dépasse le cadre des travaux de révision. Il s'agit essentiellement d'aspects liés à la sécurité des produits et de l'Internet, raison pour laquelle le Conseil fédéral propose également de réaliser le postulat dans le cadre des travaux du groupe d'experts « Avenir du traitement et de la sécurité des données ».
- Postulat Schwaab 14.3782 «Des règles pour la mort numérique»: l'art. 12 AP-LPD prévoit d'une part un droit de consulter les données d'une personne décédée, et d'autre part permet aux héritiers d'exiger l'effacement de données d'une personne décédée. Les points principaux du postulat sont ainsi mis en œuvre. Les autres aspects seront réalisés 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 de portabilité sur les données n'est pas souhaitable dans le cadre de la révision de la LPD (cf. ch.1.6.4).
- Postulat Béglé 16.3386 « Réappropriation des données personnelles: favoriser l'autodétermination informationnelle ». L'AP-LPD ne prévoit pas de concrétiser le droit de se réapproprier ses données personnelles pour les mêmes raisons que pour la portabilité des données (1.6.4). Cette question pourra être examinée par le groupe d'experts « Avenir du traitement et de la sécurité des données » ou dans le cadre de la « Stratégie Suisse numérique ».

8 Modifications des lois

8.1 Commentaire de l'AP-LPD

8.1.1 But, champ d'application et définitions

8.1.1.1 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[64].

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 (voir ch. 8.1.1.2).

8.1.1.2 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 de supprimer l'exception concernant les registres publics relatifs aux rapports juridiques de droit privé (l'art. 2, al. 2, let. d).

Pour le reste, l'AP-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[65].

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.

Suppression de la protection des personnes morales

L'AP-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. 28ss du code civil (CC)[66] (atteintes à la personnalité, telle que la réputation), la LCD, la loi fédérale du 9 octobre 1992 sur le droit d'auteur (LDA)[67], par les règles sur les secrets professionnels, d'affaires et de fabrication, ou, au plan constitutionnel, par l'art. 13 Cst reste inchangée. Cette modification 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[68]. 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. 5 AP-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 s'est montrée en faveur de la suppression de la protection des données personnelles des personnes morales[69]. Enfin, notons que le Conseil national a refusé de donner suite à une

---

64 ATF 140 I 2, cons. 9.1.

65 Voir FF **1988** 421, 452 et MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, N 286ss.

66 RS **210**

67 RS **231.1**

68 Sur cette question, voir DRECHSLER CHRISTIAN, Plädoyer für die Abschaffung des Datenschutzes für juristische Personen, PJA 2016, p. 80ss, p. 85-86.

69 Voir la AIR, p. 46.

motion qui demandait que la protection des personnes morales soit maintenue (voir ch. 1.1.5 Motion Béglé 16.3379).

La loi du 17 décembre 2004 sur la transparence (LTrans)[70]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 de la LPD a pour conséquence que le droit d'accès à des documents contenant des informations concernant des 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). L'art. 9 LTrans ne s'applique plus en cas de documents officiels contenant des données personnelles d'une personne morale. Afin de garantir la protection des droits des personnes morales lorsqu'une demande d'accès porte sur des documents contenant des informations qui pourraient, en cas de divulgation, porter atteinte à leur sphère privée, l'AP modifie certaines dispositions de la LTrans (ch. 8.2.5).

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 de l'AP-LPD mais peuvent, le cas échéant, invoquer la LTrans pour consulter des documents officiels susceptibles de contenir des informations les concernant.

Al. 2 : Exceptions au champ d'application

L'al. 2 AP-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[71] (let. b). Par ailleurs, la let. d reprend l'exception concernant le CICR, en précisant que cette dernière vaut pour tous bénéficiaires institutionnels selon l'art. 2, al. 1 de la loi sur l'Etat hôte[72], qui jouissent en Suisse d'une immunité de juridiction. Notons ici que le CICR est exclu du champ d'application de la LPD également en raison de son assimilation à une organisation internationale.

Let. c : Exceptions pour les autorités judiciaires fédérales indépendantes

L'art. 2, al. 2, let. c, AP-LPD prévoit que les traitements de données personnelles effectués par des autorités judiciaires fédérales indépendantes dans le cadre de leurs activités juridictionnelles sont exclus du champ d'application de la loi.

Cette exception est d'une part justifiée par le fait que les autorités judiciaires indépendantes ne sauraient être soumises à la surveillance du préposé pour leurs activités juridictionnelles sans que cela porte atteinte au principe de la séparation des pouvoirs et à l'indépendance de la justice. D'autre part, elle se justifie par le fait que les droits des parties et des participants à la procédure sont dans ce cas exclusivement régis pas le droit de procédure applicable (par ex. s'agissant du droit d'accès), qui offre une protection équivalente à celle de la LPD. Cela vaut aussi pour le droit des parties à avoir connaissance des données découlant de la procédure, le droit de faire rectifier certaines données ainsi que pour le traitement de données dans le cadre de la procédure judiciaire en général. Le droit procédural ne règle ainsi pas uniquement le déroulement de la procédure, mais aussi la protection de la personnalité des parties dont les données sont collectées dans le cadre de la procédure. Le droit procédural régit par ailleurs aussi les données de procédures closes. Ces dernières, dans la mesure où elles doivent converger avec les résultats de la procédure judiciaire, ne peuvent être modifiées que selon les règles de procédure applicables. Afin que le dossier ne puisse être modifié subséquemment par des instruments étrangers à la procédure, le droit procédural prévoit ainsi des moyens particuliers (rectification, interprétation, révision). Le critère déter-

70 RS **152.3**

71 FF 1988 II 449

72 RS **192.12**

minant pour juger de l'application de la LPD, en particulier en cas de procédure close, est au final l'existence ou non d'un lien direct avec une procédure. Il en résulte a contrario que la LPD est applicable aux traitements de données opérés par les services administratifs de ces autorités, tels que les services du personnel[73]. Ces traitements sont donc soumis à la surveillance du préposé.

Contrairement au droit actuel, le Conseil fédéral propose de recourir à la notion d « activités juridictionnelles » et plus à celle de « procédure pendante », qui ne convient pas à tous les types de procédure. La notion de « litispendance » ne s'applique ainsi notamment qu'aux aux procédures civiles.

La notion d' « autorité judiciaire indépendante » vise par exemple le Ministère public de la Confédération, la justice pénale militaire ou les autorités de recours indépendantes au sens de l'art. 47 de la loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[74]. L'exception ne vise pas les autorités cantonales, dans la mesure où les traitements effectués par ces dernières sont régis par le droit cantonal, sous réserve des dispositions spéciales de droit fédéral. Si des données sont traitées dans le cadre d'une procédure par une autorité qui ne peut pas être qualifiée « d'autorité judiciaire indépendante », l'exception prévue à l'al. 2, let. c ne s'applique pas. Ainsi, dans le domaine de la procédure pénale, les traitements de données effectués par les autorités fédérales de police sont régis par l'AP-LPD, sous réserve des dispositions de protection des données prévues par des lois spéciales. Il en va de même des traitements de données effectués par les autorités fédérales dans le cadre d'une procédure pénale administrative. Enfin, il convient de relever que la nouvelle teneur de l'art. 2, al. 2, let. c, AP-LPD n'a aucune conséquence sur les procédures administratives de première instance au sens de la PA. Celles-ci sont soumises à l'AP-LPD comme c'est le cas aujourd'hui.

Abrogation de l'exception pour les registres publics (art. 2, al. 2. let. d LPD)

Le Conseil fédéral considère que cette norme n'est pas compatible avec les exigences de l'art. 3 du P-STE 108. La modification ne concerne que les registres publics de droit privé tenus par les autorités fédérales soit Infostar, Zefix, le registre des aéronefs de l'Office fédéral de l'aviation civile, et le registre des marques de l'Institut de la propriété intellectuelle. 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 soit toutefois pas empêcher l'application uniforme et juste du droit privé fédéral. L'abrogation de l'art. 2, al. 2, let. d, LPD n'a ainsi de conséquences pour les registres suivants, qui relèvent de la compétence des cantons.

- Le registre foncier. En vertu des dispositions fédérales du droit du registre foncier (art. 942ss CC, art. 955 CC ainsi que l'ordonnance du 23 septembre 2011 sur le registre foncier [ORF][75]), les offices du registre foncier de chaque canton doivent tenir des registres fonciers et sont responsables de la tenue correcte de ces registres (art. 955 CC).
- Le registre des bateaux (art. 1 et 4 de l'ordonnance du 16 juin 1986 sur le registre des bateaux [ORF][76]). L'ORF est applicable à la tenue du registre des bateaux, à moins que la législation fédérale sur le registre des bateaux n'en dispose autrement.
- Les registres cantonaux du commerce. En vertu de l'art. 927 du code des obligations (CO)[77], chaque canton doit posséder un registre du commerce et désigner les organes chargés de la tenue du registre ainsi qu'une autorité cantonale chargée d'exercer la surveillance administrative sur l'office du registre du commerce (art. 3 et 4, al. 1, de l'ordonnance du 17 octobre 2007 sur le registre du commerce[78]).

[73] Voir déjà FF 1988 II 450

[74] RS **172.0121**

[75] RS **211.432.1**

[76] RS **747.111**

[77] RS **220**

[78] RS **221.411**

- Les registres concernant la poursuite pour dettes et faillites (art. 8, al. 1, de la loi du 11 avril 1889 sur la poursuite pour dettes et la faillite[79]).
- Le registre public sur les pactes de réserves de propriété (art. 715 CC).

Al. 3 : Tribunaux fédéraux

L'al. 3 de l'art. 2 AP-LPD prévoit que la loi ne s'applique pas aux traitements de données personnelles effectués par les tribunaux fédéraux dans le cadre de leurs activités juridictionnelles. Cette exception est justifiée par les mêmes motifs que celle concernant les autorités judiciaires fédérales indépendantes (voir le commentaire relatif à l'art. 2, al. 2, let. c).

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 (art. 3, al. 3, 2ème phrase). 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, les tribunaux fédéraux ont initié la création d'une surveillance indépendante. Le choix de sa forme et de sa structure relève de leur compétence, et est encore en discussion.

Al. 4 : Surveillance sur l'Assemblée fédérale et le Conseil fédéral

L'alinéa 4, reprend, s'agissant de la surveillance du préposé sur le Conseil fédéral, l'actuel art. 27, al. 1, 2ème phrase LPD. L'AP-LPD prévoit de soumettre l'Assemblée fédérale à la même règle.

Champ d'application territorial

L'AP-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[80]).

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 celle évoquées dans son rapport du 11 décembre 2015 sur la responsabilité des fournisseurs de services Internet[81]. Il convient plutôt de favoriser la conclusion de traités bilatéraux ou multilatéraux d'entraide judiciaire prévoyant la 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 États qui accueillent le siège social d'exploitants de plateformes bien connus, tels que les Etats-Unis ou l'Irlande. Enfin, le Conseil fédéral relève que l'obligation d'élection de domicile est prévue par la PA ainsi que par la loi du 17 juin 2005 sur le Tribunal administratif fédéral[82].

---

79 RS **281.1**

80 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, cons. 3.3 (« Google Street View »)).

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

82 RS **173.32**

8.1.1.3 Art. 3 Définitions

Let. a : Données personnelles

La définition des données personnelles ne subit pas de modification par rapport au droit actuel. Il s'agit de toutes les informations qui se rapportent à une personne identifiée ou identifiable. Est réputée identifiable la personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Comme c'est le cas actuellement, une possibilité purement théorique qu'une personne soit identifiée n'est pas suffisante. Il convient de prendre en compte l'ensemble des moyens raisonnablement susceptibles d'être utilisés pour identifier la personne. Le caractère raisonnable des moyens en question doit être évalué en regard des coûts et du temps nécessaire à leur utilisation. Compte tenu des technologies toujours plus pointues, et en constante évolution, il est à prévoir que la frontière entre les données personnelles et les autres données s'atténue. Des données pour lesquelles il n'existe aujourd'hui qu'une simple possibilité théorique d'identification pourront peut-être demain être attribuées à une personne déterminée.

Il convient ici de préciser que l'AP-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. Sinon, lorsqu'il est question de données, ce sont de toutes les données dont il est question, qu'elles soient personnelles ou non (par ex. en cas de profilage).

Let. c : Données personnelles sensibles

La notion de « données personnelles sensibles » (let. c) – abrégée « données sensibles » dans le texte français – est élargie aux données génétiques (ch. 3) et aux données biométriques identifiant un individu 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. k de la loi fédérale sur l'analyse génétique humaine du 8 octobre 2014[83]).

Par données biométriques, on entend ici les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne, qui résultent d'un traitement technique spécifique et permettent ou confirment son identification unique. Il s'agit par exemple des images faciales ou des données dactyloscopiques. Les photographies ne tombent ainsi dans la définition des données biométriques que lorsqu'elles sont traitées par un moyen technique spécifique permettant l'identification ou l'authentification unique d'un individu.

Comme dans la convention STE 108 (art. 6 par. 1) la directive (UE) 2016/680 (art. 10) et le règlement (UE) 2016/679 (art. 9), les données sensibles comprennent aussi les données concernant la vie sexuelle de la personne concernée. Ces dernières sont comprises dans la notion de sphère intime.

Let. d : Traitement

La définition de « traitement » (let. d) n'est pas non plus 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 du P-STE 108, 4, par. 1 du règlement (UE) 2016/679 et 3 par. 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).

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

[83] RS **810.12**

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.

Le terme de « profil de la personnalité » 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 1992, cette notion n'a pas ou peu été appliquée et semble aujourd'hui dépassée par l'évolution technologique. Cette définition est remplacée dans l'AP-LPD par celle de « profilage », que l'on trouve aussi à l'art. 3 par. 4 de la directive (UE) 2016/680 et à l'art. 4, par. 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 profilage désigne une forme particulière de traitement, et constitue donc un processus dynamique. Ce dernier est par ailleurs toujours orienté vers une finalité particulière. Le profilage se définit ainsi comme toute exploitation de données, personnelles ou non, qui consiste à analyser ou prédire les caractéristiques personnelles essentielles d'une personne. L'AP-LPD mentionne comme exemple de caractéristiques essentielles le rendement au travail, la situation économique, la santé, la sphère intime, ou les déplacements. L'analyse de ces caractéristiques peut par exemple avoir pour but de déterminer si une personne est indiquée pour une certaine activité.

La définition légale englobe l'exploitation de données personnelles et non personnelles et tient ainsi compte du fait qu'avec les technologies actuelles (telles le Big Data), l'analyse de données sans lien avec une personne fasse émerger des données personnelles. Il est sans importance que celui qui procède au profilage le fasse pour lui ou pour le compte d'un tiers. Il importe également peu que l'analyse des données soit automatisée ou non (pour la délimitation avec la décision individuelle automatisée, voir ch. 8.1.3.3). Le degré d'automatisation du traitement (par ex. avec ou sans algorithme) n'est en effet pas un critère approprié pour définir quelles activités nécessitent une protection particulière de la personne concernée. Ce qui est déterminant c'est que les données permettent d'apprécier et de prédire des caractéristiques essentielles. De cette manière le remplacement de la notion de profil de la personnalité par celle de profilage n'entraîne pas de lacune dans la protection des personnes concernées. Par ailleurs, la nouvelle définition permet de mieux cibler la base légale à conférer aux organes fédéraux. Seuls ceux qui procèdent effectivement à du profilage doivent en recevoir la compétence.

Les données issues d'un profilage sont en principe des données personnelles au sens de l'art. 3, let. a AP-LPD, qui, selon les circonstances, peuvent aussi constituer des données sensibles.

Let. h : Responsable du traitement

L'AP-LPD prévoit d'introduire cette notion, afin d'user de la même terminologie que celle du P-STE 108 (art. 2 let. b), de la directive (UE) 2016/680 (art. 3 ch. 8) et du règlement (UE) 2016/679 (art. 4 ch. 7). Par « responsable du traitement », on entend la personne privée ou l'organe fédéral qui détermine les finalités, les moyens et l'étendue du traitement des données. Deux critères cumulatifs doivent être remplis pour que l'on ait affaire à un « responsable du traitement »: la personne privée ou l'organe fédéral doit déterminer d'une part dans quels buts les données sont traitées et d'autre part par quels moyens. Cette définition se distingue ainsi partiellement de celle de « maître du fichier » qui n'implique pas la réalisation de la seconde condition. Le critère déterminant n'est plus de savoir qui décide du contenu du fichier mais des moyens du traitement des données envisagé.

Let. i : 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 celles 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. 394ss CO), d'un contrat d'entreprise (art. 363ss CO) voire encore d'un con-

trat mixte selon les obligations du sous-traitant. Un employé soumis à un contrat de travail n'est pas un sous-traitant vis-à-vis de son employeur.

Définitions non modifiées

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

Définitions abrogées

Maître du fichier : cette notion est remplacée par celle de « responsable du traitement ».

Fichier : l'AP-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, par lequel on va chercher des données dans différents serveurs afin d'évaluer des aspects de la personnalité d'un individu. Selon le droit actuel, ces activités, de même que le profilage, 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 ce type de situations 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[84].

Loi au sens formel : l'AP-LPD propose de supprimer cette définition car elle est superflue.

8.1.2 Dispositions générales de protection des données

8.1.2.1 Art. 4 Principes

Al. 1 et 2 : Licéité et proportionnalité

Les al. 1 et 2 relatifs aux principes de licéité, de bonne foi et de proportionnalité restent inchangés, sous réserve d'une modification rédactionnelle concernant la version française de l'al. 2.

Al. 3 : Finalité et reconnaissabilité

L'al. 3 regroupe les principes de finalité et de reconnaissabilité actuellement contenus aux alinéas 3 et 4 de la loi. Pour mieux aligner le droit fédéral au texte du P-108 (art. 5, ch. 4, let. b), l'AP-LPD prévoit que les données doivent être collectées pour des finalités déterminées et clairement reconnaissables pour la personne concernée. Cette nouvelle formulation n'implique pas de changements matériels par rapport au droit en vigueur : la collecte des données et les finalités du traitement doivent être reconnaissables. Tel est en principe le cas lorsque l'on informe la personne concernée, que 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 sont pas admis. Cette qualité s'apprécie selon les circonstances, 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'AP-LPD, toujours dans un but de rapprochement terminologique avec les textes européens (art. 5, par. 4, let. b du P-STE 108, art. 4, par. 1, let. b de la directive [UE] 2016/680 et 5, par. 1, let. b du règlement [UE] 2016/679), prévoit dans le même alinéa que les données ne peuvent être traitées ultérieurement de manière incompatible avec les finalités initiales. Tel est le cas lorsque le traitement ultérieur peut légitimement être considéré par la personne concernée comme inattendu, inapproprié ou contestable. On peut citer les cas suivants :

- l'utilisation à des fins publicitaires d'adresses obtenues lors de la récolte de signature pour une campagne politique ;

[84] MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, n° 563; BELSER URS, in: Maurer-Lambrou/Vogt (éds.), Basler Kommentar, Datenschutzgesetz, 2ème éd., Bâle 2006, Art. 3 LPD n° 32; VPB 62.57.

- 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) ;
- 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[85] ;
- la collecte par une entreprises privée d'adresses IP de titulaires de raccordement offrant au téléchargement des œuvres piratées[86].

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 (online 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[87]. 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.

Selon l'al. 4, les données ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées au-delà de la durée nécessaire aux finalités du traitement. En d'autres termes, dès que le but du traitement le permet, les données ne doivent plus être conservées telles quelles, mais uniquement de manière à ce qu'elles ne permettent plus d'identifier les personnes concernées. Cette exigence découle déjà du principe de proportionnalité (art. 4, al. 2 LPD). Le Conseil fédéral propose toutefois de la mentionner expressément, afin de s'aligner sur le texte du P-STE 108 (art. 5, par. 1, let. e), ainsi qu'à la directive (UE) 2016/680 (art. 4, par. 1, let. e) et au règlement (UE) 2016/679 (art. 5, par. 1, let. e). Notons que certaines finalités impliquent parfois de conserver les données telles quelles très longtemps. Cela vaut par exemple pour les archives fédérales, dont les tâches légales impliquent justement de à conserver des données personnelles pendant de longues périodes.

Al. 5 : Exactitude

L'al. 5 de l'AP-LPD reprend le principe de l'exactitude des données figurant actuellement à l'art. 5 LPD. Cette modification permet de regrouper les grands principes de base dans une seule disposition, comme le font les textes européens (art. 5 du P-STE 108, art. 4 de la directive (UE) 2016/680 et 5 du règlement (UE) 2016/679). Elle n'implique pas de changement matériel. Ainsi, celui qui traite des données personnelles doit, comme c'est le cas aujourd'hui, examiner si les données sont correctes et actuelles. Lorsque tel n'est pas le cas, les données doivent être effacées. Ces devoirs valent en principe pour tous les types de traitement et tous les auteurs de traitements, dans la mesure où ces derniers ont, tout comme la personne intéressée, un intérêt prépondérant à ce que seules des données actuelles et pertinentes soient traitées.

Ces devoirs doivent 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 ; LBNS[88]). 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.

---

85 JAAC 69.106, cons. 5.6.

86 ATF 136 II 508, cons. 4.

87 MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, n° 731.

88 RS **432.21**

Pour terminer, par souci de se rapprocher de la terminologie des textes européens, 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. Il est aussi précisé que les données doivent être actuelles. Cela n'entraîne aucune modification matérielle, dans la mesure où aujourd'hui déjà, les données doivent être mises à jour et complétées autant que les circonstances le requièrent[89].

Al. 6 : Consentement

La première phrase prévoit que le consentement, lorsqu'il est exigé pour justifier un traitement de données, n'est valable que s'il est donné librement, clairement, et après que la personne a été dûment informée. Cette nouvelle formulation permet de se rapprocher de la terminologie du P-STE 108 (art. 5 par. 2), et du règlement (UE) 2016/679 (art. 4, ch. 11 et 6, ch. 1, let. a). Comme aujourd'hui, le consentement doit être donné pour un traitement précis ou une catégorie de traitements, et couvrir l'ensemble de ses finalités. Avec cette formulation, le consentement reste libre de toute règle de forme, et peut être donné par actes concluants pour autant qu'il soit clair. En revanche, la simple inaction de la personne concernée n'est pas constitutive de consentement.

Selon la seconde phrase de l'al. 6 AP-LPD, le consentement doit être exprès lorsque le traitement concerne des données sensibles ou consiste en du profilage. L'AP-LPD remplace ainsi, 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 ». Cette modification permet de mettre fin aux controverses doctrinales concernant la qualité du consentement[90], et de remplir les exigences de la convention STE 108 (art. 5 al. 2). Le règlement (UE) 2016/679 prévoit une règle similaire (art. 4, ch. 11 et 6, ch. 1, let. a). Le consentement exprès doit résulter d'une déclaration écrite (y compris par voie électronique) ou orale, ou encore de signes. Cela pourrait se faire notamment en cochant une case ou en cliquant sur un bouton (par ex. « suivant ») sur un site Internet, en optant pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration.

8.1.2.2 Art. 5 Communication de données personnelles à l'étranger

Cette disposition correspond aux exigences de l'art. 12 du 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). Le par. 3 définit les cas dans lesquels cette condition est réalisée. L'art. 5 permet aussi de se rapprocher des exigences du droit de l'Union européenne (art. 45 et ss du règlement (UE) 2016/679).

Al. 1 : Principe

L'al. 1 reprend le même principe que celui fixé à l'art. 6, al. 1, LPD, en supprimant toutefois les termes « du fait de l'absence *d'une législation assurant* un niveau de protection adéquat ». Il s'agit d'une modification purement rédactionnelle, rendue nécessaire par le nouvel al. 2.

Al. 2 : Constatation de l'adéquation par le Conseil fédéral

En vertu de l'al. 2, 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. 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

[89] MEIER PHILIPPE, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, n° 753s. Voir aussi FF **1988 421,** 457

[90] Certains auteurs opposent le terme « explicite » aux actes concluants, alors que d'autres estiment qu'un consentement explicite peut résulter d'actes concluants si l'intention de la personne concernée est claire. Pour un résumé des avis sur cette question voir : VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015.

protection adéquat[91]. 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)[92]. Afin de garantir une application uniforme de l'al. 2, le niveau de protection de la législation d'un Etat étranger est dorénavant examiné par le Conseil fédéral. Celui-ci établit une liste des Etats disposant d'une législation assurant un niveau de protection adéquat (al. 7). 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. Le résultat de cet examen est publié sous la forme d'une ordonnance du Conseil fédéral, qui est publiée au Recueil officiel. 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 pas sur la liste 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 les exigences pour qu'il puisse constater un niveau de protection adéquat. Avec la révision, la liste 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 comme un moyen auxiliaire mis à la disposition des maîtres du fichier qui envisagent de communiquer des données à l'étranger.

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

Al. 3 : Absence de décision du Conseil fédéral

En l'absence d'une décision du Conseil fédéral au sens de l'al. 2, l'al. 3, let. a à d prévoit que des données personnelles peuvent être communiquées à l'étranger, si un niveau « approprié » de protection des données personnelles est garanti. A l'instar du droit de l'Union européenne, l'AP-LPD recourt à deux termes différents aux al. 2 et 3. Le terme « adéquat » est réservé pour qualifier la législation de l'Etat étranger.

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, 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. 56, let. b AP-LPD.

L'al. 3, let. b et c correspond aux exigences de l'art. 12 par. 3 let. b du P-STE 108 qui prescrit qu'un niveau de protection des données approprié peut être assuré par des garanties ad hoc et standardisées agrées, établis 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 prévoit une réglementation analogue à l'art. 46. Il en va de même pour la directive (UE) 2016/680 (art. 37).

Al. 3, let. b : Garanties spécifiques

En vertu de l'al. 3 let. b, des données peuvent être transférées à l'étranger si des garanties assurent dans un cas particulier une protection des données appropriée, et si ces dernières ont été préalablement communiquées au préposé. Si le préposé a des objections, il en informe le responsable du traitement ou le sous-traitant dans un délai de 30 jours à compter de la réception des garanties (al. 4). L'OLPD prévoit le même délai à l'art. 6, al. 5. A défaut d'objections ou passé ce délai, le responsable du traitement est en droit de communiquer des données à l'étranger. 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 garanties. Il reste également responsable du préjudice qui pourrait résulter d'une violation des garanties prévues.

---

91 FF **2003** 1940-1941

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

Comme cela ressort de la terminologie, la notion de « garanties spécifiques » vise un cas « spécifique » de communication de données à l'étranger, et non des communications effectuées sous une forme standardisée. Dans le secteur privé, il peut s'agir de clauses contractuelles convenues dans le cadre d'un contrat entre le responsable du traitement et le destinataire. Dans le secteur public, l'organe fédéral peut, lorsqu'il accorde sa coopération à un Etat étranger, lui fixer des conditions à respecter en matière de protection des données. Contrairement aux garanties standardisées (voir let. c), les garanties spécifiques ne valent que pour les communications prévues dans ledit contrat. Si le responsable du traitement envisage une nouvelle communication de données, il doit en principe fixer de nouvelles garanties.

Al. 3, let. c : Garanties standardisées

En vertu de l'al. 3, let. c, des données peuvent être communiquées à l'étranger moyennant des garanties standardisées. Ces garanties peuvent être élaborées soit par les personnes privées ou les milieux intéressés (ch. 1) soit établies ou reconnues par le préposé (ch. 2). Les organes fédéraux peuvent également recourir à ce type de garanties. La notion de « garanties standardisées » 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 cas prévu à l'al. 3, let. c, ch. 1, les garanties 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 du P-STE 108. Le préposé dispose d'un délai de six mois pour communiquer au responsable du traitement s'il approuve ou non les garanties élaborées (al. 5, 1ère phrase). Ce délai commence à courir à partir du moment où le préposé a reçu un dossier complet, c'est-à-dire toutes les informations nécessaires pour se prononcer sur la validité des garanties standardisées annoncées. Il s'agit d'un délai d'ordre ; en cas de non-respect, les règles sur le déni de justice sont applicables. Le responsable du traitement ne peut pas communiquer des données à l'étranger avant d'avoir obtenu une décision du préposé susceptible de recours (art. 5 PA).

En vertu de l'al. 3, let. c, ch. 2, le responsable du traitement peut également recourir aux garanties standardisées établies ou reconnues par le préposé, par exemple des contrats-modèles ou des clauses standards, et doit l'en informer (al. 6). Dès qu'il a exécuté son devoir d'information, il est en droit de communiquer des données à l'étranger. Le responsable du traitement qui décide de communiquer des données à l'étranger moyennant des garanties standardisées au sens de l'al. 3, let. c, est 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 garanties notamment par le destinataire des données. Il convient de prévoir dans l'ordonnance une obligation pour le préposé de publier une liste des garanties standardisées établies ou reconnues, comme le prévoit du reste le droit en vigueur (art. 6, al. 3, OLPD).

Al. 2, let. d : Règles d'entreprises contraignantes

En vertu de l'al. 3, let. d, des données peuvent être communiquées à l'étranger moyennant des règles d'entreprise contraignantes qui ont été préalablement approuvées par le préposé (ch. 1) ou par une autorité chargée de la protection des données à l'étranger (ch. 2). Cette disposition remplace l'art. 6, al. 2, let. g, LPD. L'al. 2, let. d se rapproche du droit de l'Union européenne qui 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'entreprises est prévue à l'art. 57, par. 1 let. s du règlement (UE) 2016/679. L'al. 3, let. d constitue un renforcement du droit en vigueur dans la mesure où les règles d'entreprise contraignantes doivent être approuvées. Le préposé dispose d'un délai de six mois pour communiquer à la société concernée s'il approuve ou non les règles d'entreprise contraignantes qui lui ont été soumises (al. 5). Pendant ce laps

de temps, aucune donnée ne peut être transmise à l'étranger. La décision du préposé est susceptible de recours.

Si les règles d'entreprise contraignantes ont été approuvées par une autorité chargée de la protection des données à l'étranger (al. 3, let. d, ch. 2), l'entreprise établie en Suisse doit les communiquer au préposé de telle manière que ce dernier puisse effectuer ses tâches de surveillance (al. 6). Ces dispositions répondent au besoin des groupes d'entreprises situées dans différents pays.

Les instruments visés à l'al. 3, let. d 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 mises 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'entreprises contraignantes.

Al. 7 : Publication de la liste

La liste du Conseil fédéral est publiée (al. 7). Il conviendra de préciser dans la future d'ordonnance d'exécution qu'elle devra être mise à jour régulièrement. En d'autres termes, le Conseil fédéral devra régulièrement évaluer si les législations des Etats figurant sur cette liste. La violation de l'art. 5 est sanctionnée pénalement (art. 50, al. 2, let. b et 51, al. 1, let. a AP-LPD).

8.1.2.3 Art. 6 Communication exceptionnelle de données personnelles à l'étranger

Al. 1

A l'instar du droit en vigueur (art. 6, al. 2, LPD), l'art. 6, 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 du P-STE 108 et à l'art. 49 du règlement (UE) 2016/679. La directive (UE) 2016/680 prévoit une réglementation analogue à l'art. 38.

La let. a correspond à l'art. 6, al. 2, let. b, LPD. Le consentement de la personne concernée est valable si les conditions de l'art. 4, al. 6 AP-LPD sont respectées. Celle-ci doit en particulier être informée sur les risques du transfert.

La let. b correspond à l'art. 6, al. 2, let. c, LPD.

La let. c, ch. 1 correspond à l'art. 6, al. 2, let. d, 1ère phrase LPD. 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 correspond 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 une autorité judiciaire ou administrative ».

La let. d précise que la communication peut être nécessaire non seulement pour protéger la vie ou l'intégrité corporelle 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. En raison de l'abrogation de l'art. 2, al. 2, let. d, LPD concernant les registres publics relatifs aux rapports juridiques de droit privé, il est nécessaire de préciser que l'exigence d'un niveau de protection adéquat n'est pas applicable lors-

qu'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

L'al. 2 prévoit que une obligation pour le responsable du traitement ou le sous-traitant de communiquer au préposé les communications de données personnelles effectuées en vertu de l'al. 1, let. b, c et d. Cette disposition vise aussi bien le secteur privé que le secteur public. Elle met en œuvre l'exigence prévue à l'art. 12 par. 5 du P-STE 108.

La violation de l'art. 6 est poursuivie sur plainte en vertu de l'art. 51, al. 1, let. a AP-LPD.

8.1.2.4 Art. 7 Sous-traitance

Les al. 1, 2, et 4 introduisent des modifications terminologiques, rendues nécessaires par les nouvelles définitions (sous-traitant, responsable du traitement).

L'al. 2 est complété en ce sens que le responsable du traitement doit s'assurer que le sous-traitant est en mesure de garantir non seulement la sécurité des données, mais aussi les droits de la personne concernée. Cette extension est exigée par la directive (UE) 2016/680 (art. 22 par. 1). Le Conseil fédéral estime qu'une transposition uniquement sectorielle dans les domaines Schengen ne fait pas de sens ceci d'autant plus que le règlement (UE) 2016/679 (art. 28 par. 1) prévoit la même chose. Le Conseil fédéral peut préciser, par voie d'ordonnance, les autres obligations du sous-traitant.

L'al. 3 est nouveau et prévoit que le sous-traitant ne peut lui-même sous-traiter un traitement qu'avec l'accord écrit préalable du responsable du traitement. Il peut s'agir d'un accord général. Dans ce cas le sous-traitant informe le responsable du traitement de tout changement (ajout ou remplacement d'autres sous-traitants) lui permettant ainsi d'émettre des objections à l'encontre de ces changements. Il s'agit là d'une exigence de la directive (UE) 2016/680, pour les domaines Schengen (art. 22 par. 2). Le règlement (UE) 2016/679 prévoit une règle similaire (art. 28 par. 2). Le Conseil fédéral a fait le choix de l'appliquer à tous les cas de sous-traitance, ce qui permet de renforcer la transparence des traitements ainsi que la maîtrise des personnes concernées sur leurs données. Par ailleurs, le responsable du traitement est tenu d'informer la personne concernée lorsqu'un traitement est confié à un sous-traitant, et doit lui communiquer les données ou catégories de données personnelles concernées (art. 13, al. 4, AP-LPD).

8.1.2.5 Art. 8 Elaboration de recommandations de bonnes pratiques

Le caractère général et technologiquement neutre des règles de la LPD est susceptible d'entraîner, dans le secteur privé surtout, une grande incertitude quant aux comportements à adopter, pour les responsables du traitement et les sous-traitants, mais aussi pour les personnes concernées. Le Conseil fédéral estime qu'il est impératif de disposer de règles plus concises et dynamiques pour concrétiser la loi. Il propose dès lors de formaliser l'élaboration et l'adoption de recommandations de bonnes pratiques. Ces dernières permettent d'avoir des solutions plus précises dans des secteurs qui suscitent aujourd'hui de nombreuses questions tels que la vidéosurveillance, le Cloud-computing ou les réseaux sociaux, de préciser certaines notions, tels que le risque accru (art. 16 AP-LPD), les modalités de certains droits tel que le droit d'être consulté en cas de décision individuelle automatisée (art. 15 et 20, al. 3 AP-LPD), ou les modalités de certains devoirs tels que le devoir d'information (art. 13 et 14 AP-LPD) et le devoir d'effectuer une analyse d'impact du traitement (art. 16 AP-LPD). Les recommandations peuvent être édictées à l'attention du secteur privé, mais aussi à l'attention du secteur public.

L'élaboration de codes de conduite et la promotion de l'autorégulation par les Etats mais aussi par l'autorité de contrôle sont aussi prévues par le règlement (UE) 2016/679, à ses art. 40 et 57 par. 1 (let. m).

Al. 1 : Elaboration par le préposé

L'al. 1 prévoit que le préposé édicte des recommandations de bonnes pratiques. L'idée de confier cette tâche à une commission extra-parlementaire a été écartée durant les travaux préparatoires (voir ch. 1.6.5). Il apparaît en effet que le préposé est le plus à même, compte tenu de sa structure et de son expérience, à assumer cette tâche avec efficacité. Les recommandations peuvent concrétiser certains aspects de la loi, concernant notamment la transparence des traitements, les droits des personnes concernées et les obligations des responsables du traitement et du sous-traitant.

Il s'agit ici de formaliser et de développer une activité que le préposé effectue déjà partiellement dans le cadre de ses tâches actuelles d'information et de conseil (art. 28, 30 et 31 LPD). Lors de l'élaboration de ces recommandations, le préposé doit intégrer les différents milieux intéressés, tels que l'économie, les fédérations de consommateurs ou encore les patients. Le préposé doit également 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.

Al. 2 : Elaboration par les milieux intéressés

L'al. 2 prévoit que les responsables du traitement ainsi que les milieux intéressés peuvent aussi élaborer des recommandations de bonnes pratiques ou compléter, respectivement modifier celles du préposé. Ils peuvent ensuite les faire approuver par ce dernier. Le préposé approuve la recommandation soumise s'il estime que les dispositions de protection des données – qui peuvent aussi figurer dans d'autres textes législatifs que l'AP-LPD – sont respectées. 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. De telles solutions seraient particulièrement bienvenues dans le domaine de l'Internet (protection des données dans l'exploitation de réseaux sociaux, utilisation de cookies etc.) où la seule régulation étatique est bien souvent insuffisante pour protéger les droits des personnes concernées.

Dans le domaine de l'Internet et des télécommunications, les milieux intéressés ont adopté des « codes » 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 dans ce domaine. 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[93], qui prévoit certaines obligations pour ses signataires concernant le blocage de certains sites internet, 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)[94] 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.

Al. 3 : Publication

L'al. 3 prévoit que les recommandations de bonnes pratiques sont publiées par le préposé. La publication peut se faire sur son site Internet.

8.1.2.6 Art. 9 Respect des recommandations de bonnes pratiques

Lorsque le responsable du traitement ou le sous-traitant se conforme aux recommandations de bonnes pratiques, il respecte par là-même les dispositions qu'elles concrétisent (art. 9, al. 1, AP-LPD). Cette disposition met en évidence que le respect des recommandations correspond matériellement à celui de la loi. Elle clarifie ainsi la nature de ces dernières, dont le rôle est de concrétiser la loi.

L'al. 2 prévoit que les dispositions de protection des données peuvent être respectées d'une autre manière que celle prévue par les recommandations de bonnes pratiques. Il souligne le

93 https://asut.ch/asut/resources/documents/initiative_sectorielle_protection_jeunesse_m%C3%A9dias.pdf.

94 http://simsa.ch/_Resources/Persistent/2260a505424ef1e0c8100899a6f38a06e4a4ecff/130201-simsa-cch-public-f.pdf.

caractère facultatif de ces dernières. Notons que les milieux concernés sont libres, sur le plan associatif par exemple, de rendre les recommandations obligatoires.

8.1.2.7 Art. 10 Certification

L'art. 10 de l'AP-LPD règle la certification facultative, qui figure actuellement à l'art. 11 LPD. L'AP-LPD étend l'objet de la procédure de certification à toutes les opérations de traitement. En plus des systèmes (procédures et organisation) et des produits (programmes, logiciels, systèmes), il est maintenant possible de faire certifier des services Cette extension permet de se rapprocher du règlement (UE) 2016/679, qui prévoit lui aussi une certification pour toutes les opérations de traitement (art. 42).

La procédure d'accréditation des organismes de certification indépendants par le Service d'accréditation suisse, qui y associe le préposé, demeure inchangée[95].

8.1.2.8 Art. 11 Sécurité des données

L'art. 11 AP-LPD correspond à l'art. 7 LPD, avec quelques modifications rédactionnelles. 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). Il est précisé que les responsables du traitement et les sous-traitants doivent protéger les données personnelles contre tout traitement non autorisé et toute perte, par des mesures organisationnelles et techniques appropriées. La notion de perte englobe aussi celle de destruction des données.

Ce devoir peut, selon les situations, se traduire par différentes mesures. Il peut s'agir de pseudonymiser et chiffrer des données. Il peut aussi s'agir de prévoir des garanties pour assurer la confidentialité, l'intégrité et la disponibilité des systèmes et des services de traitement, et pour rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique. Enfin, il peut encore s'agir d'élaborer des procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

8.1.2.9 Art. 12 Données personnelles d'une personne décédée

Plusieurs éléments de cette norme figurent actuellement à l'art. 1, al. 7, OLPD. La possibilité de consulter les données personnelles d'une personne décédée est vue comme un droit partiel inclus dans le droit d'accès. Il s'agit pourtant d'un droit de la personne concernée, qui ne peut le faire valoir que pour les traitements de données la concernant. La disposition de l'ordonnance étend ainsi le droit d'accès aux tiers, qui peuvent obtenir des informations sur les données d'une tierce personne sans qu'une base légale ne l'autorise. Cela pose un problème qui est résolu par l'ajout d'une telle norme dans la loi. D'un point de vue systématique, la norme en question est détachée de l'article régissant le droit d'accès, qui concerne uniquement la personne concernée, et est ajoutée à la section fixant les dispositions générales de protection des données.

En plus de régler le droit d'accès aux données personnelles d'une personne décédée, l'art. 12 satisfait en partie au postulat Schwaab 14.3782 « Des règles pour la "mort numérique" », en prévoyant un droit à l'effacement ou la destruction des données de la personne décédée par les héritiers. La possibilité d'une « mort numérique » existe donc désormais, sauf dans les cas où des intérêts prépondérants de tiers ou de la personne concernée s'y opposent ou que cette dernière l'aura expressément interdit. D'autres questions soulevées dans le postulat, concernant par exemple la possibilité d'hériter les données, seront traitées dans le cadre de la révision du droit des successions.

Al. 1 : Consultation

L'al. 1 dispose que le responsable du traitement accorde la consultation gratuite des données personnelles d'une personne décédée en cas d'intérêt légitime. Dans certains cas cet intérêt est présumé (al. 2, voir ci-dessous). La simple curiosité ne constitue en revanche pas

[95] 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 235.13)

intérêt pertinent. Parallèlement à l'art. 12 AP-LPD, la révision du droit des successions prévoit un droit de consultation limité aux personnes pouvant fait valoir une prétention successorale. Ce droit leur permet de faire valoir leurs droits patrimoniaux dans le cadre de la dévolution (art. 601a AP-CC).

Afin de tenir compte de la volonté de la personne décédée, il est prévu que la consultation doit être refusée lorsque celle-là l'a expressément interdite de son vivant (let. a). La consultation est aussi refusée lorsqu'il existe les intérêts du défunt l'en empêchent (let. b). Cela faut en particulier pour les données sensibles contenues dans des dossiers médicaux ou par des avocats. Aucun secret de fonction ou professionnel ne peut toutefois être invoqué.

La consultation est aussi refusée lorsqu'elle irait à l'encontre d'intérêts prépondérants de tiers (let. b). Les intérêts de la proche parenté au sens de l'art. 1, al. 7, OLPD sont compris dans les intérêts des tiers. Ces intérêts englobent aussi la protection de la personnalité des tiers. Leur caractère prépondérant est décidé au cas par cas, compte tenu du but de la consultation, de l'importance des données pour la personne qui demande à les consulter et du risque qu'elle ait en même temps accès à des données d'un tiers.

Al. 2: Présomption d'un intérêt légitime

L'al. 2 présume un intérêt légitime chez les personnes en lien de parenté directe avec le défunt ou qui sont mariées, en partenariat enregistré ou en concubinage avec lui au moment du décès. Il suffit donc que la personne concernée démontre avoir un tel lien avec le défunt pour qu'elle n'ait pas à démontrer avoir un intérêt légitime à consulter les données.

La pesée d'intérêts au sens de l'al. 1, let. a et b n'est pas influencée par cette présomption.

Al. 3 : Secret de fonction ou professionnel

L'al. 3 lève en principe le secret de fonction et le secret professionnel qui pourraient être invoqués contre une demande de consultation des données. Cela signifie, par exemple, qu'un médecin ne pourrait pas se prévaloir du secret médical pour interdire à un fils de consulter les données médicales concernant son père.

Si le détenteur d'un secret de fonction ou d'un secret professionnel a ses propres intérêts à préserver, ceux-ci pourront être pris en compte dans la pesée effectuée au sens de l'al. 1, let. b.

Al. 4 : Effacement

L'al. 4 dispose que chaque héritier peut exiger que le responsable du traitement efface ou détruise les données personnelles du défunt gratuitement. Ce droit est volontairement limité aux héritiers. C'est aussi à dessein que la possibilité d'exiger une telle mesure est accordée à chaque héritier, sans qu'il doive consulter l'ensemble des membres de l'hoirie, ce qui poserait d'innombrables problèmes de procédure. En cas d'intérêts divergents des héritiers, une pesée sera effectuée. Enfin, le droit d'exiger l'effacement reste valable même après la dissolution de l'hoirie, une fois la succession réglée.

L'effacement ou la destruction doit être refusée si le défunt les a expressément interdites de son vivant ou qu'ils vont à l'encontre d'intérêt prépondérants de ce dernier ou de tiers.

On peut faire valoir le droit d'exiger l'effacement vis-à-vis du responsable du traitement indépendamment de toute violation de la personnalité ou de tout traitement illicite des données.

Al. 5

L'al. 5 réserve les dispositions spéciales d'autres lois fédérales. Cette disposition réserve par exemple la LTrans qui règle l'accès à des documents officiels de l'administration fédérale ou encore la loi fédérale du 26 juin 1998 sur l'archivage[96] qui prévoit des dispositions spéciales concernant le délai de protection des données personnelles contenues dans des documents qui ont été archivés auprès des archives fédérales.

[96] RS **152.1**

8.1.3 Obligations du responsable du traitement et du sous-traitant

La section 3 porte sur les obligations du responsable du traitement et du sous-traitant. Ces dernières valent tant pour les personnes privées que les organes fédéraux.

8.1.3.1 Art. 13 Devoir d'informer lors de la collecte de données

L'art. 13 AP-LPD regroupe les art. 14 et 18a 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 du 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 uniquement 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, un 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 but de la révision.

Al. 1 : Principe

Selon l'al. 1, le responsable du traitement doit informer activement la personne concernée de la collecte de données personnelles, et ce même si elles sont obtenues auprès d'un tiers. Il doit l'informer de façon active. 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. L'information peut être transmise individuellement ou collectivement, dans les conditions générales ou au moyen d'une déclaration standard s'affichant sur un site Internet, par exemple. Il est possible de recourir à des symboles ou à des pictogrammes, pour autant qu'ils contiennent les éléments nécessaires. Les informations peuvent aussi être données en plusieurs paliers (par ex. un clic de souris sur un symbole fait apparaître des informations détaillées). Si l'on opte pour une information générale, elle doit être facilement accessible, complète et aisément identifiable. La personne concernée doit y être rendue attentive sans intervention de sa part, c'est-à-dire sans qu'elle doive la chercher ou la demander. 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 de l'identité et des coordonnées du responsable du traitement, des données ou catégories de données traitées et des finalités du traitement. La base juridique du traitement doit aussi être communiquée – notamment par les organes fédéraux – pour permettre à la personne concernée de faire valoir ses droits. L'association d'une disposition générale définissant les principes de base d'agissant des informations à communiquer (1ère phrase) 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. 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 recommandations de bonnes pratiques adaptées à leur domaine. La personne concernée doit être informée au plus tard au moment de la collecte des données personnelles, sauf dans le cas visé à l'al. 5.

Al. 3 : Communication de données personnelles à des tiers

Lorsque les données personnelles sont communiquées à des tiers, le responsable du traitement doit informer la personne concernée des destinataires ou des catégories de destinataires. S'il connaît leur identité, il doit la lui communiquer. Ce devoir vaut aussi lorsque le destinataire se trouve à l'étranger.

Al. 4: Sous-traitance

L'al. 4 prévoit que lorsqu'un traitement est confié à un sous-traitant, le responsable du traitement communique à la personne concernée son identité et ses coordonnées ainsi que les données ou les catégories de données personnelles concernées. Cette obligation vaut aussi lorsque le sous-traitant se trouve à l'étranger.

Al. 5 : Moment de la communication

L'al. 5 arrête le moment où la personne concernée doit être informée lorsque les données personnelles ne sont pas collectées auprès d'elle. L'information doit lui parvenir au plus tard lors de leur enregistrement ou lors de la première communication à des tiers. Le terme « enregistrement » ne couvre pas uniquement le processus technique d'insertion dans un système informatique, mais toute activité consécutive à la collecte, qui prépare une nouvelle utilisation des données personnelles.

Le non-respect de l'obligation d'informer est sanctionné (voir l'art. 50, al. 1, let. a et b, ch. 1 et 2 AP-LPD).

8.1.3.2 Art. 14 Exceptions au devoir d'informer

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

Al. 1 et 2 : Exceptions au devoir d'informer

Selon l'al. 1, le responsable du traitement est délié de son devoir d'information lorsque la personne concernée dispose déjà des informations au sens de l'art. 13. Tel est par exemple le cas lorsqu'elles lui ont été transmises auparavant, et que les nouvelles informations à transmettre sont identiques. On considérera aussi que la personne concernée est déjà informée lorsqu'elle a elle-même rendu les informations accessibles. Il est toutefois probable dans ce cas que l'exigence de transparence du traitement implique qu'on lui communique d'autres informations au sens de l'art. 13 AP-LPD.

Selon l'al. 2, l'obligation d'informer ne s'applique pas pour les données personnelles qui n'ont pas été collectées auprès de la personne concernée, si l'enregistrement ou la communication est expressément prévue par la loi (al. 2, let. a), ou si le devoir d'informer est impossible à respecter ou nécessite des efforts disproportionnés (al. 2, let. b). 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.

Al. 3 et 4 : Limitation de l'information

Les al. 3 à 4 fixent les conditions auxquelles le responsable du traitement peut renoncer à la communication des informations, la restreindre ou la différer. A cet effet, il procède à une pesée d'intérêts dont les modalités différeront selon que ce dernier est un particulier ou un organe fédéral. 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.

L'al. 3 autorise le responsable du traitement à restreindre ou à différer la communication des informations ou à y renoncer si une loi au sens formel le prévoit (let. a). On songe ici princi-

palement à des normes de droit public à l'attention d'organes fédéraux. Les particuliers sont concernés dans une moindre mesure. Le devoir d'informer peut également être limité si les intérêts prépondérants d'un tiers l'exigent (let. b). 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.

L'al. 4 règle des situations dans lesquelles certains responsables du traitement peuvent restreindre ou différer la communication des informations ou y renoncer. Un responsable du traitement privé peut selon la let. a 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.

Un organe fédéral peut, en vertu de la let. b, 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 risque de compromettre une enquête, une instruction ou une procédure administrative ou judiciaire (ch. 2). Il s'agit d'éviter que la loi sur la protection des données ne permette de contourner les dispositions des codes de procédures régissant tel que le droit d'être entendu, et de faire échouer des procédures administratives ou judiciaires.

Al. 5 : Disparition du motif de limitation

Selon l'al. 5, le responsable du traitement doit communiquer les informations dès que le motif justifiant le refus, la restriction ou l'ajournement disparaît. Fait exception le cas où la communication est impossible ou nécessite un travail disproportionné (voir le commentaire relatif à l'al. 2).

8.1.3.3 Art. 15 Devoir d'informer et d'entendre la personne concernée en cas de décision individuelle automatisée

L'art. 15 AP-LPD prévoit l'existence d'un devoir d'informer et d'entendre la personne concernée en cas de décision individuelle automatisée. Cette disposition remplit les exigences de l'art. 8, let. a du P-STE 108 et de l'art. 3, par. 3 et 11 de la directive (UE) 2016/680. Les art. 4, par. 3 et 22 du règlement (UE) 2016/679 contiennent une disposition similaire. L'introduction de la notion de décision individuelle automatisée est nécessaires car ces décisions sont de plus en plus fréquentes, dans tous les domaines de l'économie, et reposent parfois sur des données fausses.

Al. 1: Information

Selon l'al. 1, le responsable du traitement doit informer la personne concernée de l'existence d'une décision individuelle automatisée lorsque cette dernière a des effets juridiques pour elle ou l'affecte de manière significative. Il doit être clair pour la personne concernée qu'elle fait l'objet d'une telle décision.

Il y a une décision individuelle automatisée lorsqu'une exploitation de données a lieu sans intervention humaine, et qu'il en résulte une décision, respectivement 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. Une décision individuelle automati-

sée a des effets juridiques pour la personne concernée lorsqu'elle influe directement sur sa position juridique. Pour qu'elle l'affecte de manière significative, il faut que la décision individuelle automatisée produise des effets concrets qui soient d'une certaine gravité. Les exemples sont nombreux. On peut par exemple penser aux conditions selon lesquelles une personne peut conclure un contrat de leasing (par ex. intérêts, durée du contrat, délais de paiement) qui dépendent uniquement de l'examen automatisé de sa situation financière. On peut aussi penser à l'assurance-maladie qui, sur la base d'une évaluation des données de santé de la personne concernées par un algorithme, refuse de conclure un contrat avec elle. Les amendes en matière de circulation routière, qui sont envoyées automatiquement au conducteur sur la base d'une prise de vue, sont également des décisions individuelles automatisées.

Une décision individuelle automatisée peut également reposer sur un profilage au sens de l'art. 3, let. f AP-LPD. Il ne s'agit toutefois pas d'une condition. Les deux notions ne se recoupent ainsi pas entièrement. Le critère central pour les différencier est celui de l'automatisation : un profilage ne doit pas forcément résulter d'un processus automatisé. Un autre critère réside dans les effets sur la personne concernée. Pour la décision individuelle automatisée, il faut qu'il en résulte certaines conséquences concrètes pour la personne concernée, alors que tel n'est pas le cas pour le profilage. Les données sont analysées en vue d'un but déterminé, mais il n'est pas nécessaire que cette analyse ait des effets directs sur la personne concernée.

Al. 2 : Audition

Selon l'al. 2, le responsable du traitement doit donner à la personne concernée la possibilité de faire valoir son point de vue sur la décision individuelle automatisée et sur les données traitées. Combiné avec le devoir d'information, cette audition garantit que la personne concernée n'est pas soumise à des décisions prises sans aucune intervention humaine. Elle doit avoir notamment la possibilité de donner son avis concernant la décision prise et les données qui y ont conduit. Le but est entre autres d'éviter que la personne concernée ne subisse des conséquences juridiques ou matérielles du fait d'un traitement 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 lorsque il refuse de conclure un contrat avec une personne parce que cette dernière est qualifiée par erreur de non-solvable. L'obligation d'informer et d'entendre la personne concernée n'a toutefois pas d'effet sur la liberté contractuelle. Lorsque le responsable du traitement ne permet pas à la personne concernée faire valoir son point de vue, cette dernière peut faire valoir son droit par le biais du droit d'accès de l'art. 20 AP-LPD.

La loi ne fixe pas le moment auquel l'information et l'audition doivent avoir lieu. En conséquence, la personne concernée peut être informée et entendue 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, pour autant qu'il n'en résulte pas de frais supplémentaires (par ex. des frais de procédure) pour elle.

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 individuelle automatisée est prévue par la loi. Pour les organes fédéraux, il s'agira d'une loi au sens de celles visées à l'art. 27 de l'AP-LPD.

Le non-respect de l'obligation d'informer est sanctionné (voir l'art. 50, al. 1, let. a et b, ch. 1 et 2 AP-LPD).

8.1.3.4 Art. 16 Analyse d'impact du traitement

L'art. 16 AP-LPD instaure une obligation de procéder à une analyse d'impact du traitement. Cette disposition concrétise les exigences posées à l'art. 8bis, al. 2, du 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 du traitement résultent de l'al. 2. 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 réduire 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.

L'introduction de l'analyse d'impact du traitement ne présente aucune nouveauté pour les organes fédéraux, dans la mesure où ces derniers doivent aujourd'hui déjà annoncer les projets impliquant des traitements automatisés de données aux conseillers à la protection des données, respectivement au préposé (art. 20 OLPD). Le processus de la méthode de gestion de projets Hermès devrait largement correspondre aux exigences de l'étude d'impact.

Al. 1 : *Motifs justifiant la réalisation d'une étude d'impact du traitement*

L'al. 1 prévoit que le responsable du traitement (ou le sous-traitant) procède à une analyse d'impact du traitement envisagé lorsque ce dernier est susceptible d'entraîner un risque accru pour la personnalité et les droits fondamentaux de la personne concernée. 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 et 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 l'autodétermination de la personne concernée, de même que sa dignité et son identité[97]. 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 accru lorsqu'il apparaît que les propriétés du traitement envisagé ont ou pourraient avoir pour effet de restreindre considérablement la liberté de la personne de disposer de ses données. Tel est notamment le cas lorsque le traitement concerne un grand volume d'informations étroitement liées à la personnalité, qui permettent d'identifier la personne et qui en révèlent certaines caractéristiques. Le risque accru peut par exemple découler de la nature des données traitées ou de leur contenu (données personnelles sensibles par ex.), de la nature et du but du traitement (profilage par ex.), de la quantité de données traitées, de leur transmission dans d'autres pays (en l'absence d'une protection appropriée par ex.) ou du fait qu'elles sont accessibles à un grand nombre de personnes, voire à tout le monde. D'autres indices d'un risque accru résident dans le fait qu'en cas d'utilisation abusive des données, celles-ci pourraient porter atteinte à la personnalité, à la dignité ou au bien-être de la personne. Une surveillance systématique

[97] Voir DIGGELMANN OLIVER, in: Waldmann/Belser/Epiney (édit.), Basler Kommentar, Bundesverfassung, Bâle 2015, ad art. 13 Cst. n° 7.

de la personne et de son comportement (courriels échangés par ex.) ou de l'espace public (une place animée par ex.) peut aussi représenter un risque accru. Lorsque le traitement envisagé est susceptible d'engendre une risque accru, une analyse d'impact doit être faite.

Al. 2 : Contenu

Selon l'al. 2, l'étude d'impact du traitement doit tout d'abord exposer le traitement envisagé. Il faut ainsi présenter les différents processus, le but du traitement ou la durée de conservations des données personnelles. Par ailleurs, l'étude d'impact doit montrer quels risques le traitement implique pour la personnalité et les droits fondamentaux de la personne concernée. Il s'agit ici d'une estimation, qui doit déjà être faite en amont, lors de l'examen de la nécessité de procéder à une étude d'impact. Il convient ainsi de présenter le risque qu'engendre le traitement envisagé, et comment l'évaluer. Enfin, l'étude d'impact doit expliquer par quelles mesures ces risques sont réduits. Il s'agira souvent de mettre en œuvre les principes de l'art. 4 AP-LPD, ainsi que les principes de protection dès la conception et par défaut (privacy by design/by default ; art. 18 AP-LPD). A cette occasion, il faut faire une balance entre les intérêts de la personne concernée et ceux du responsable du traitement ou du sous-traitant. Cette balance d'intérêts doit être intégrée à l'étude d'impact du traitement et motivée en conséquence.

Al. 3 : Communication au préposé

Selon l'al. 3, le responsable du traitement (ou le sous-traitant) doit communiquer au préposé les résultats de l'analyse d'impact ainsi que les mesures prévues pour minimiser les risques d'atteinte à la personnalité et aux droits fondamentaux de la personne concernée. Cette information ne figure pas dans P-STE 108, mais elle correspond à la réglementation de l'Union européenne (art. 28 de la directive [UE] 2016/680 et art. 36 du règlement [UE] 2016/679). Elle a été incluse dans l'avant-projet pour permettre au préposé d'agir à titre préventif, dans un rôle de conseiller. L'avantage pour le responsable du traitement est qu'il est ainsi possible de prévenir à un stade précoce d'éventuels problèmes en matière de protection des données.

Al. 4 : Objections du préposé

L'al. 4 donne 3 mois au préposé dès la réception de toutes les information nécessaires pour informer le responsable du traitement s'il a des objections concernant les mesures envisagées. Après avoir reçu les résultats de l'analyse d'impact du traitement, le préposé se contente de vérifier que les mesures proposées pour protéger les droits fondamentaux et la personnalité de la personne concernée sont suffisantes. Il n'examine en revanche pas de manière approfondie le processus de traitement, puisque cet examen a déjà fait l'objet de l'analyse d'impact. Si, au bout de trois mois, le responsable du traitement n'a pas reçu de nouvelles du préposé, il peut partir du principe que ce dernier n'a pas d'objection concernant les mesures envisagées. Le préposé est cependant libre d'ouvrir ultérieurement une enquête si les conditions définies à l'art. 41 AP-LPD sont remplies. Ce peut être le cas lorsque les risques n'ont pas été évalués correctement dans le cadre de l'analyse d'impact et que les mesures prises s'avèrent insuffisantes ou manquent leur cible.

Le non-respect de l'obligation de procéder à une analyse de l'impact du traitement et d'en communiquer les résultats est sanctionné (voir l'art. 50, al. 1, let. c, et 51, al. 1, let. d, AP-LPD).

8.1.3.5 Art. 17 Notification des violations de la protection des données

L'art. 17 AP-LPD instaure l'obligation de notifier toute violation de la protection des données. Cette disposition concrétise les exigences fixées à l'art. 7, al. 2, du P-STE 108 et à l'art. 30 de la directive (UE) 2016/680. L'art. 33 du règlement (UE) 2016/679 contient une disposition similaire.

Al. 1 : Notion et fondements

L'al. 1 dispose que le responsable du traitement notifie au préposé tout traitement non autorisé de données et toute perte, à moins que la violation ne présente vraisemblablement pas de risques pour la personnalité et les droits fondamentaux de la personne concernée. Un traitement non autorisé pourra par exemple consister en un effacement non autorisé (cf. dé-

finition à l'art. 3, let. d). La violation peut être causée par un tiers, mais son auteur peut aussi être un collaborateur qui outrepasse ses compétences. Le traitement non autorisé peut entraîner une perte de contrôle de la personne concernée sur ses données ou une utilisation abusive de celles-ci. Il peut aussi engendrer une violation de la personnalité, par exemple en entraînant la divulgation d'informations que la personne concernée souhaitait garder secrètes. Pour cette raison, l'art. 23, al. 2, let. a AP-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 protection des données a été violée. C'est pourquoi le responsable du traitement doit notifier tout traitement non autorisé, au préposé en premier lieu et, si les conditions de l'al. 2 sont remplies, à la personne concernée également. La notification doit avoir lieu dès que 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 du risque créé pour la personne concernée. Plus ce risque sera élevé et le nombre de personnes concernées important, plus son intervention devra être rapide.

Le responsable du traitement ne peut renoncer à notifier la violation de la protection des données au préposé que si elle ne met vraisemblablement pas en péril la personnalité ou les droits fondamentaux de la personne concernée. Cette exception vise à éviter la notification de violations insignifiantes ; son interprétation doit cependant être restrictive. Le responsable du traitement doit évaluer les conséquences possibles de la violation pour la personne concernée. Il ne peut renoncer à l'annoncer que s'il aboutit à la conclusion qu'il est hautement improbable que le traitement non autorisé présente un risque.

Al. 2 : Annonce à la personne concernée

Selon l'al. 2, 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 et 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. 3 et 4

L'al. 3 dispose que le responsable du traitement peut restreindre, différer la notification à la personne concernée ou y renoncer dans les cas visés à l'art. 14, al. 3 et 4 (voir ch. 8.1.3.2).

Un traitement non autorisé peut aussi survenir chez le sous-traitant. Le cas échéant, l'al. 4 l'oblige à en informer le responsable du traitement. Il revient ensuite à ce dernier d'apprécier les risques et de décider si la violation doit être notifiée au préposé et à la personne concernée.

Le non-respect de l'obligation d'annoncer une violation de la protection des données est poursuivi d'office (voir l'art. 50, al. 2, let. d, AP-LPD).

8.1.3.6 Art. 18 Protection des données dès la conception et par défaut

L'art. 18 AP-LPD introduit le devoir de protection des données dès la conception, ainsi que par défaut. Cette disposition met en œuvre les exigences du P-STE 108 (art. 8, ch. 3) et 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 et au sous-traitant de prendre dès la conception les mesures appropriées permettant de prévenir et de minimiser les risques d'atteintes à la personnalité et aux droits fondamentaux de la personne concernée. 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 recommandations de bonnes pratiques moins nécessaires. Par ailleurs ces technologies sont indispensables pour mettre en

œuvre les règlementations 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. 4 AP-LPD. 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. 4 AP-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 soit traitées, et de façon à ce qu'elles soient conservées le moins longtemps possible.

L'introduction du principe de protection des données dès la conception ne devrait pas avoir de conséquences importantes pour les organes fédéraux. En effet, ses derniers sont aujourd'hui déjà tenus d'annoncer à leurs conseilleurs à la protection des données, respectivement 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 : Protection des données par défaut

Selon l'al. 2, le responsable du traitement et le sous-traitant sont tenus de prendre des mesures préalables appropriées pour garantir que, par défaut, seules sont traitées les données nécessaires à la finalité du traitement (privacy by default). Les mesures en question résident dans des réglages prédéfinis (par ex. l'installation d'un software) qui s'appliquent de manière 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, tel 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 modifier le système lui-même, elle a toujours la possibilité, s'agissant des réglages par défaut, de choisir une solution différente (voir art. 4, al. 6 AP-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 et le sous-traitant peuvent montrer, par une certification ou une étude d'impact du traitement notamment, qu'ils respectent les obligations définies à l'art. 18 AP-LPD. Le non-respect des obligations définies à l'art. 18 est sanctionné (voir l'art. 51, al. 1, let. e, AP-LPD).

8.1.3.7 Art. 19 Autres devoirs

L'art. 19 AP-LPD prescrit d'autres obligations pour le responsable du traitement ou le sous-traitant.

Let. a : Devoir de documentation

L'art. 19, let. a, oblige le responsable du traitement et le sous-traitant à documenter leurs traitements de données. Cette disposition concrétise l'art. 8bis, al. 1 du P-STE 108 et l'art. 25 de la directive (UE) 2016/680. L'art. 30 du règlement (UE) 2016/679 contient une disposition similaire. La nouvelle disposition remplace l'obligation faite aux privés de faire enregistrer leurs fichiers par le préposé (l'art. 36 de l'avant-projet prévoit que les organes continueront de déclarer leurs activités pour qu'elles soient enregistrées). La procédure d'annonce des fichiers est bureaucratique implique de lourdes charges administratives pour le responsable du traitement. Elle est par ailleurs peu utile, dans la mesure où la LPD prévoit pour les personnes privées plusieurs exceptions à l'obligation d'enregistrement. Le devoir de documenter le traitement des données s'applique lui à tous les processus de traitement des données. Il permet d'obtenir à peu d'efforts une documentation homogène de tous les processus privés de traitement. Une ordonnance précisera les éléments qui doivent y figurer. La documentation doit toutefois garantir que le responsable du traitement et le sous-traitant sont en mesure de remplir leurs obligations d'information et de notification. Ainsi, les violations de la protection des données selon l'art. 17 AP-LPD doivent aussi être documentées.

Le devoir de documentation joue un rôle central pour la transparence du traitement des données. Le non-respect de ce devoir est sanctionné (voir l'art. 51, let. f, AP-LPD).

Let. b : Autres devoirs d'information

La let. b prévoit que le responsable du traitement et le sous-traitant sont tenus d'informer les destinataires des données personnelles de toute rectification, effacement, destruction ou violation de la protection des données et de toute limitation du traitement selon l'art. 25, al. 2 ou 34, al. 2, AP-LPD. Cette obligation complète d'autres règles de protection des données pour les cas dans lesquels les données personnelles ont été communiquées à des tiers. Elle est prévue par l'art. 16 par. 5 de la directive (UE) 2016/680 ainsi que par l'art. 19 du règlement (UE) 2016/679. Le traitement de données non pertinentes représente en principe une violation de la personnalité, raison pour laquelle la personne qui les traite doit s'assurer que les données sont correctes (art. 4, al. 5, AP-LPD). Le fait de les effacer, les supprimer ou d'en limiter le traitement implique en principe que leur traitement n'est plus licite. L'obligation d'informer prévue ici permet d'éviter que des tiers qui n'auraient pas connaissance de ces opérations continuent de traiter les données.

Le responsable du traitement ou le sous-traitant peut renoncer à la communication si celle-ci s'avère impossible ou si elle exige des efforts disproportionnés. Cette exception est à interpréter de manière restrictive. Avant de considérer qu'une communication n'est pas possible ou qu'elle ne l'est qu'au prix d'efforts démesurés, le responsable du traitement ou le sous-traitant doit au moins avoir tenté d'informer les destinataires et s'être heurté à des obstacles concrets particulièrement difficiles à surmonter. Pour juger du caractère disproportionné, on tiendra compte par ailleurs du contenu de la communication à faire. Plus la rectification, l'effacement ou la limitation est déterminante pour la protection de la personne concernée, plus les efforts du responsable ou du sous-traitant pour informer les destinataires devront être importants.

8.1.4 Droits de la personne concernée

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

8.1.4.1 Art. 20 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, qu'une personne mineure ou une personne interdite 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 quel nul ne peut renoncer par avance au droit d'accès (art. 20, al. 6 AP-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

Selon l'al. 2, la personne concernée reçoit d'abord les informations qui doivent lui être communiquées en vertu du devoir d'informer (voir l'art. 13, al. 2 à 4 AP-LPD). Il s'agit principalement des informations qui sont nécessaires pour que celle-ci puisse faire valoir ses droits et pour que le traitement des données soit transparent. Les informations prévues aux let. a à g doivent dans tous les cas lui être communiquées. Il s'agit de l'identité et des coordonnées du responsable du traitement (let. a), des données traitées (let. b) et de la finalité du traitement (let. c). La personne concernée doit également être informée de la durée de la conservation des données ou, si cela n'est pas possible, les 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. 4 AP-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. Le droit d'accès lui permet par ailleurs de savoir s'il existe une décision individuelle automatisée (let. e), auquel cas les informations prévues à l'al. 3 doivent également lui être fournies. Enfin, la personne concernée reçoit les informations disponibles sur l'origine des données (let. f), comme le prévoit déjà le droit en vigueur.

Al. 3 : Communication en cas de décision individuelle automatisée

Lorsque, à l'issue d'un traitement de données, une décision à l'égard de la personne concernée est prise, l'al. 3 prévoit qu'elle doit recevoir des informations supplémentaires sur le résultat de cette décision, la manière dont elle a été prise ainsi que sur les conséquences et sa portée. On pense ici en particulier aux décisions individuelles automatisées portant sur l'octroi d'un crédit ou d'une assurance, basées uniquement sur l'analyse de données relatives à la situation financière ou à la santé d'une personne (voir ch. 8.1.3.3). Les informations dont il est question ici vont au-delà de celles prévues à l'art. 15 AP-LPD. Celle-ci doit pouvoir comprendre comment la décision a été prise et quelles sont les conséquences pour elle. Le responsable du traitement doit ainsi lui communiquer quelles données ont été prises en compte et quelle importance elles ont eues sur la décision.

Le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements conformément à l'art. 21. Les personnes privées peuvent également faire valoir des intérêts personnels tels que la protection de leurs secrets d'affaires, auquel cas il faut procéder à une pesée des intérêts. Ainsi, le responsable du traitement n'a pas à révéler à la personne concernée l'algorithme utilisé pour la prise de la décision et peut invoquer la protection des secrets d'affaires. Toutefois, il doit motiver le résultat de la décision de manière à permettre à la personne concernée de savoir sur la base de quelles données le résultat en question a été obtenu. La personne concernée doit par ailleurs connaître les effets de la décision sur sa position juridique ou sur sa situation concrète et les conséquences y relatives. Par ailleurs, si la personne concernée n'a eu connaissance d'une décision individuelle automatisée que lors de l'exercice de son droit d'accès, elle doit avoir la possibilité d'exprimer son avis (voir l'art. 15, al. 2, AP-LPD).

Al. 4 et 5

Selon l'al. 4, le responsable du traitement peut communiquer à la personne concernée des données sur sa santé par l'intermédiaire d'un médecin qu'elle a désigné. Cette disposition est tirée du droit en vigueur et n'a subi qu'une modification rédactionnelle.

L'al. 5 a fait l'objet de quelques modifications rédactionnelles. Le responsable du traitement reste en principe tenu de fournir les renseignements demandés lorsque le traitement est effectué par un sous-traitant.

Le non-respect des obligations définies à l'art. 20 AP-LPD est sanctionné (voir l'art. 50, al. 1, let. a, AP-LPD).

8.1.4.2 Art. 21 Restriction au droit d'accès

L'al. 1 dispose que le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements pour les mêmes motifs que ceux prévus à l'art. 14, al. 3 et 4, AP-LPD. Nous renvoyons au commentaire de l'art. 14 (voir ch. 8.1.3.2). Les motifs d'une restriction au droit d'accès sont les mêmes que dans le droit actuel, mais l'avant-projet les rattache au devoir d'informer la personne concernée.

Si le responsable du traitement refuse, restreint ou diffère la communication des informations, il doit en indiquer le motif (al. 2). Il peut uniquement faire valoir les motifs définis à l'art. 14, al. 3 et 4. En cas de restriction du droit d'accès, les organes fédéraux doivent rendre une décision sujette à recours. Aucune procédure formelle n'est prévue pour les personnes privées. Pour des motifs de preuve, celles-ci devraient toutefois communiquer par écrit les motifs à la personne concernée. La disposition de l'al. 2, 2ème phrase est nouvelle: l'organe fédéral n'est pas tenu d'indiquer le motif si cela est susceptible de porter atteinte aux intérêts mentionnés à l'art. 14, al. 4, let. b, AP-LPD. Cette disposition empêche que l'indication des motifs ne révèle ce que la restriction du droit d'accès vise à protéger.

L'indication du motif doit permettre à la personne concernée de vérifier si l'information a été légitimement refusée, restreinte ou différée. Toutefois, le niveau de cette exigence peut être moins élevé lorsqu'il existe un risque de collusion avec le motif de la restriction du droit d'accès.

8.1.4.3 Art. 22 Restriction au droit d'accès applicable aux médias

L'art. 22 AP-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 la promotion de l'entreprise de média[98]. Le média doit en outre avoir un caractère périodique. On considère comme média à caractère périodique les journaux, les revues, les entreprises de radio et de télévision, les agences de presse et les services d'information on line remis 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[99].

8.1.5 Dispositions particulières pour le traitement de données par des personnes privées

La section 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 (voir l'art. 35, al. 1 et 3, Cst.). Les trois dispositions de cette section sont à considérer ensemble: l'art. 23 AP-LPD règle les atteintes à la personnalité lors du traitement des données, l'art. 24 AP-LPD définit les motifs justifiant de telles atteintes et l'art. 25 AP-LPD règle les droits que les victimes d'un traitement ayant porté atteinte à leur personnalité peuvent faire valoir. L'avant-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 vis-à-vis, en particulier dans le secteur privé. Ce comportement est mis sur le compte des craintes concernant le coût que peut avoir un procès[100], craintes qui ont incité à revoir la répartition des coûts en procédure civile (voir le ch. 8.2.9).

---

[98] BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2ème éd., Berne 2011, n°1769

[99] BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2ème éd., Berne 2011, n°1420

[100] Voir les p. 90 ss et 219 du document „Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz“ du 10 mars 2011.

8.1.5.1 Art. 23 Atteintes à la personnalité

L'art. 28 CC ne définit pas la notion d'atteinte à la personnalité. L'art. 23 AP-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.

Al. 2 : Fictions d'atteintes à la personnalité

L'al. 2 se réfère notamment au respect des principes applicables aux traitements des données et prévoit quatre 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. 4, 5, 6 et 11. 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 explicitement 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, du P-STE 108. Selon la let. c, il y a également atteinte à la personnalité lorsque des données sensibles sont transmises à des tiers. Enfin, le fait d'effectuer un profilage sans le consentement exprès de la personne concernée constitue également une atteinte à la personnalité.

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[101]. Cette modification vise uniquement à améliorer la clarté ; elle est conforme 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 cas où l'atteinte est licite. L'AP-LPD regroupe les motifs justificatifs à l'art. 24.

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. 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 personnelles ne peut être violée. Toutefois, cette disposition n'a une portée que si le traitement a lieu conformément aux dispositions légales, soit dans le respect des principes visés aux art. 4, 5, 6 et 11.

8.1.5.2 Art. 24 Motifs justificatifs

L'art. 24 définit les motifs qui rendent licites les traitements de données portant 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. Aucune pesée des intérêts n'est en principe prévue dans le cas où la personne concernée donne son consentement ou que le motif justificatif est prévu par la loi. Une telle pesée est en revanche nécessaire pour établir si l'intérêt public ou privé est bien prépondérant. Cet examen met en ba-

[101] Voir à cet égard l'ATF 136 II 508, consid. 5.2.3.

lance d'une part l'intérêt de la personne concernée à préserver sa liberté de disposer de ses données personnelles notamment, et d'autre part l'intérêt de l'auteur du traitement. L'atteinte ne sera licite que si l'intérêt au traitement des données l'emporte sur l'intérêt de la personne concernée à disposer de ses données.

Al. 2 : Intérêts prépondérants de la personne qui traite des données personnelles

Cette disposition précise dans quels cas les intérêts prépondérants de la personne qui traite des données personnelles entrent en considération. Cette liste correspond pour l'essentiel à celle en vigueur et n'est pas exhaustive. Elle mentionne diverses finalités qui justifient un traitement des données et qui peuvent l'emporter sur l'intérêt de la personne concernée. Schématiquement, elle comprend trois catégories de traitements : ceux réalisés à des fins économiques, ceux réalisés pour le compte des médias et ceux réalisés à des fins non liées à la personne, de recherche par exemple. Dans certains cas, la finalité du traitement ne suffit pas à elle seule pour justifier une atteinte à la personnalité. Le traitement doit respecter certaines conditions supplémentaires afin que le motif justificatif d'un intérêt prépondérant puisse le cas échéant être invoqué. Il s'agit principalement des let. b, c, e et f. Dans ces cas, il y a lieu en premier lieu d'examiner si le traitement en question respecte les conditions légales avant de procéder à une pesée des intérêts en cause.

Al. 2, let. c : Traitement dans le but d'évaluer le crédit de la personne concernée

Cette disposition introduit le critère de la majorité. Elle vise à protéger les mineurs, comme le veut la révision. Cette modification devrait avoir une portée limitée vu que la capacité de contracter des personnes mineures est restreinte. Des cas d'abus sont néanmoins possibles comme l'a révélé la procédure ouverte par le préposé contre l'entreprise Moneyhouse[102].

Al. 2, let. e : Traitements à des fins de recherche

Le motif justificatif prévu à l'al. 2, 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 le Big Data 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, celles-ci doivent être anonymisées. Ce principe résulte déjà de l'art. 4, al. 4 AP-LPD. Une violation de cette règle constitue une atteinte à la personnalité selon l'art. 23, al. 2, let. a qui peut être justifiée par un des motifs prévus à l'art. 24. En vertu de la nouvelle disposition prévue à l'art. 24, al. 2, let. e, AP-LPD, il n'est dorénavant plus possible de justifier une violation de l'art. 4, al. 4 AP-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. 23, al. 2, let. a AP-LPD qui peut être justifiée par un des motifs prévus à l'art. 24. 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.

8.1.5.3 Art. 25 Prétentions

L'art. 25 définit les prétentions que la personne concernée peut faire valoir contre des personnes privées.

[102] Voir : https://www.edoeb.admin.ch/datenschutz/00626/00747/01022/index.html?lang=fr. La procédure est encore pendante.

Al. 1 : 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, il détermine les prétentions spécifiques que la personne concernée peut faire valoir. Par souci de clarté, l'AP-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. 28a, al. 1, ch. 1 et 2, CC en matière de protection des données. En vertu de l'al. 1, 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 (let. b). Enfin, elle peut exiger la rectification, 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, l'avant-projet propose de le prévoir expressément. Cela correspond aux exigences de l'art. 8, let. e, du 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[103]. Une décision analogue à celle rendue par la Cour de justice européenne[104] contre Google serait donc également possible en Suisse. Le droit à l'oubli n'est toutefois pas absolu[105]. La jurisprudence 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.

Al. 2 : Mention du caractère litigieux

L'al. 2 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. Le demandeur peut par ailleurs dans ce cas exiger que le traitement des données personnelles soit limité. La limitation des données satisfait aux exigences de l'art. 16, par. 3, de la directive (UE) 2016/680. Le règlement (UE) 2016/679 prévoit une règle similaire (art. 18). Le P-STE 108 ne prévoit en revanche pas un tel droit. La limitation du traitement signifie que les données contestées sont marquées de façon à ce que leur utilisation reste limitée à ce qui est nécessaire pour constater leur exactitude, respectivement leur inexactitude. Le marquage doit être clair. Cela peut consister à déplacer temporairement les données sélectionnées vers un autre système de traitement, à rendre les données personnelles sélectionnées inaccessibles aux utilisateurs, ou à retirer temporairement les données publiées d'un site internet. Dans les systèmes de traitements informatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques afin que les données ne fassent pas l'objet de traitements ultérieurs et ne puissent pas être modifiées.

Al. 3: Communication à des tiers ou publication

L'al. 3 prévoit, comme c'est déjà le cas aujourd'hui, que la rectification 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. 28a, 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, qui figure désormais à l'art. 243, al. 2, let. a CPC[106].

[103] Voir en particulier ATF **109** II 353 ; ATF **111** II 209 et ATF **122** II 449.

[104] Voir jugement Rs. C-131/12 (Google Spain SL, Google Inc./Agencia Española de Protección de Datos (AEPD), Mario Costeja González) du 13.5.2014, ECLI:EU:C:2014:317.

[105] ATF **111** II 209 consid. 3c

[106] RS **272**

8.1.6 Dispositions particulières pour le traitement de données par les organes fédéraux

8.1.6.1 Art. 26 Organe responsable et contrôle

Par rapport à l'art. 16 LPD, l'art. 26 subit quelques modifications. A l'al. 1 supprime pour des raisons rédactionnelles « dans l'accomplissement de ses tâches ».

L'al. 2 supprime les termes « de manière spécifique » pour les mêmes motifs. Il prévoit en outre 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.

8.1.6.2 Art. 27 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, l'AP-LPD prévoit de régler le niveau de la base légale pour les traitements de données sensibles, des profilages ou la prise d'une décision individuelle automatisée à l'al. 2 et d'autre part d'énumérer les exceptions relatives à l'exigence d'une base légale (al. 3).

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.

Al. 2 : Base légale dans une loi au sens formel

L'al. 2 précise que la base légale doit être prévue dans une loi au sens formel s'il s'agit de traitements de données sensibles, de profilage ou d'une prise de décision individuelle automatisée au sens de l'art. 15, al. 1 AP-LPD. Toutefois, une base légale au sens matériel suffit si deux conditions cumulatives sont remplies. La première (let. a) prescrit que le traitement doit être indispensable à l'accomplissement d'une tâche clairement définie dans une loi au sens formel. Pour que cette condition soit applicable, 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. 2, let. b) est nouvelle. Elle présente l'avantage de limiter de manière plus précise la portée de la seconde phrase de l'al. 2, 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.

Al. 3 : Exceptions

Cette disposition prévoit des exceptions à l'exigence d'une base légale au sens des al. 1 et 2. Ainsi, un organe fédéral peut exceptionnellement traiter dans un cas d'espèce et sans base légale des données personnelles si l'une des conditions prévues aux let. a à c est réalisée. La let. a vise une décision du Conseil fédéral autorisant un organe fédéral à traiter dans un cas d'espèce des données personnelles sans base légale. Cette décision n'est pas susceptible de recours. En vertu de la let. b, les organes fédéraux peuvent également traiter des données si la personne concernée a donné son consentement au sens de l'art. 4, al. 6, AP-LPD ou si elle a rendu ses données personnelles à tout un chacun et ne s'est pas opposée expressément au traitement. 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 exceptionnellement 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.

8.1.6.3 Art. 28 Traitements de données dans le cadre d'essais pilotes

Les modifications apportées à l'art. 17a 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. 17a LPD peuvent être fixées dans la future ordonnance d'exécution.

Les conditions fixées aux al. 1 et 2 sont identiques à celles de l'art. 17a, al. 1, LPD sous réserve que la notion de « profils de la personnalité » est remplacée par celle de «profilage ». De plus, il est précisé à la let. c qu'une phase d'essai est nécessaire, « en particulier pour des raisons techniques ». Cette modification est due à la suppression l'art. 17a, 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 certaines modifications rédactionnelles.

8.1.6.4 Art. 29 Communication de données personnelles

L'art. 29 AP-LPD ne modifie pas le principe fixé à l'art. 19 LPD selon lequel les organes fédéraux ne sont en droit en principe 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. 27, al. 1 et 2, AP-LPD. Il résulte de cette précision que l'art. 29 ne renvoie pas aux exceptions prévues à l'art. 27, al. 3. 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. 29, al. 2, let. a à e, AP-LPD.

La notion de « données personnelles » de l'al. 1 vise également les données sensibles. Les exceptions prévues à l'al. 2, let. a à e, sont dès lors 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. 27, al. 3, let. c AP-LPD (voir ch. 8.1.6.2).

L'art. 29, al. 3 AP-LPD 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 à l'art. 29, 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'art. 29, al. 3, AP-LPD, le terme « auch » (qui n'existe pas dans la version française) par celui de « zudem / en outre » et de le placer en début de phrase afin de montrer explicitement que l'al. 3 constitue une base légale supplémentaire à celles prévues à l'al. 1.

L'art. 29, al. 4 ne subit pas de modification par rapport à l'art. 19, al. 2, LPD.

Par contre, l'exigence de base légale pour les « procédures d'appel » dans le secteur public est abandonnée (art. 19, al. 3, LPD), car d'une part elle rompt le caractère technologiquement neutre de la LPD et d'autre part elle est dépassée à l'ère de la société numérique.

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

8.1.6.5 Art. 30 Opposition à la communication de données personnelles

Cette disposition correspond à l'art. 20 LPD, sous réserve de certaines modifications rédactionnelles.

8.1.6.6 Art. 31 Proposition des documents aux Archives fédérales

Cette disposition correspond à l'art. 20 LPD. Elle ne subit pas de modifications matérielles.

8.1.6.7 Art. 32 Traitement à des fins de recherche, de planification et de statistique

Cette disposition correspond pour l'essentiel à l'art. 22 LPD. Deux modifications sont apportées à l'al. 2 concernant les renvois aux art. 4, al. 3, 27, al. 1 et 2 et 29, al. 1 AP-LPD.

En outre 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.

8.1.6.8 Art. 33 Activités de droit privé exercées par les organes fédéraux

Cette disposition correspond à l'art. 23 LPD. Elle ne subit pas de modifications matérielles.

8.1.6.9 Art. 34 Prétentions et procédure

L'art. 34 correspond en grande partie à l'art. 25 LPD. Il subit néanmoins quelques modifications qui sont présentées ci-dessous.

Al. 2 : Mention du caractère litigieux

Cette disposition prévoit la mention du caractère litigieux d'une donnée, mesure qui a été reprise du droit en vigueur. Lorsque l'exactitude ou l'inexactitude d'une donnée ne peut pas être établie, l'organe fédéral doit ajouter la mention de son caractère litigieux. En vertu du nouvel al. 2, la personne concernée peut en outre exiger la limitation du traitement. Ce droit correspond aux exigences de l'art. 16 de la directive (UE) 2016/680. L'art. 18 du règlement (UE) 2016/679 contient une réglementation analogue. Par contre, le P-STE 108 ne prévoit pas une telle disposition. La limitation du traitement signifie que les données litigieuses doivent être marquées de telle manière qu'elles ne puissent être traitées que dans le but de constater leur exactitude ou inexactitude. 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 ou de retirer provisoirement les données d'un site Internet accessible au public. Dans des systèmes de traitement automatisé de données, la limitation du traitement devrait être garantie par des mesures techniques, de telle manière à empêcher tout traitement ultérieur ou modification des données.

Al. 3 : Prétentions

Cette disposition règle les prétentions que les personnes concernées peuvent faire valoir contre des organes fédéraux.

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. 34, al. 3, let. a et b. 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. 25 AP-LPD prévoit le même droit, de sorte que la réglementation est identique pour les responsables du traitement des secteurs privé et public (voir ch. 8.1.5.3). Cette modification ne comporte néanmoins pas de changement par rapport à la situation légale, sous réserve de l'al. 4.

Par rapport à l'art. 25, al. 3, let. a, LPD, le nouvel al. 3, let. a est modifié en sens que la dernière partie de la phrase concernant l'opposition à la communication à des tiers est supprimé. En effet ce droit est expressément régi par l'art. 30 AP-LPD[107]. Le droit de s'opposer à la communication de données personnelles en vertu de l'art. 30 n'est pas lié à un traitement illicite, contrairement aux prétentions prévues à l'art. 34. Cette modification n'a toutefois pas de conséquence en pratique. En effet, la personne concernée qui se prévaut de l'art. 34 peut

[107] Voir à ce sujet BANGERT JAN, commentaire des art. 25 et 25bis LPD, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3ème Edition, Bâle 2014, ch. 62 ss.

simultanément s'opposer à la communication de ses données personnelles en vertu de l'art. 30.

L'al. 3, 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. 30. L'art. 30 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. 4 : Fonds d'institutions patrimoniales publiques

Cette disposition prescrit que la rectification, l'effacement ou la destruction de données ne peut être exigée des bibliothèques, des établissements d'enseignement, des musées, des archives ou d'autres institutions patrimoniales publiques pour les fonds qu'elles gèrent. 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. 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. 4 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 prouver qu'elle dispose d'un intérêt prépondérant. Cette exception doit être considérée au regard de la tendance toujours plus grande de publier quantités d'archives 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 archives 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 accessible à tout un chacun des informations fausses ou constituant des atteintes à sa personnalité. Il résulte de la première phrase de l'al. 1 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.

8.1.6.10 Art. 35 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.

8.1.6.11 Art. 36 Registre des activités de traitement

Comme indiqué au commentaire de l'art. 19 AP-LPD, l'art. 11a, al. 3, LPD qui prévoit une obligation pour les personnes privées de déclarer certains fichiers au préposé est supprimée et remplacée par une obligation de documenter les traitements de données. Par contre,

l'obligation pour les organes fédéraux de déclarer leurs fichiers est maintenue, sous réserve de certaines modifications.

L'art. 36, al. 1 prévoit en effet que le préposé tient un registre des activités de traitements que les organes fédéraux lui ont préalablement annoncées. Ce registre est accessible en ligne, comme c'est le cas aujourd'hui (al. 2). L'obligation pour l'organe fédéral de déclarer une activité de traitement correspond en substance à son obligation de déclarer un fichier. Il s'agit d'une adaptation de la terminologie puisque la présente révision supprime la notion de « fichier » (art. 3, let. g, LPD). Cette nouvelle terminologie correspond également à celle de l'art. 24 de la directive (UE) 2016/680 ainsi qu'à celle de l'art. 30 du règlement (UE) 2016/679.

Si l'art. 36 s'écarte un peu des normes européennes, il aboutit en substance au même résultat. Cette disposition permet en effet au public et au préposé d'avoir une vue d'ensemble des activités de traitement des organes fédéraux. Le contenu de la déclaration correspond en grande partie à celle définie à l'art. 16 OLPD, qui doit, le cas échéant, être complétée par d'autres informations telles que celles définies à l'art. 24 de la directive (UE) 2016/680.

La charge administrative des organes fédéraux reste inchangée.

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

8.1.7.1 Art. 37 Nomination et statut

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. Quant à l'art. 53 du règlement (UE) 2016/679, il a la même teneur que l'art. 43 de la directive (UE) 2016/680.

Les al. 2, 4 et 5 ne subissent aucune modification par rapport au droit en vigueur (art. 26, al. 2, 4 et 5 LPD).

L'al. 3, 1ère 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 du P-STE 108 et de l'art. 42 par. 1 et 2 de la directive (UE) 2016/680 qui a le même teneur que l'art. 52 par. 1 et 2 du règlement (UE) 2016/679.

8.1.7.2 Art. 38 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. A noter que l'art. 54 par. 1 let e du règlement (UE) 2016/679 prévoit une règle similaire.

Dorénavant le mandat du préposé ne peut être renouvelé que deux fois. Ce dernier peut donc rester en fonction pendant 12 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. 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)[108] (art. 10 al. 1, LPers, par renvoi de l'art. 14, al. 1, LPers).

Les al. 2, 3 et 4 restent inchangés par rapport à l'art. 26a LPD.

8.1.7.3 Art. 39 Activité accessoire

L'art. 39 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 étant soumis aux dispositions de la LPers.

Alors que l'art. 26b 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

[108] RS 831.10

affectées, l'art. 39, al. 1, 1ère phrase pose le principe selon lequel le préposé ne peut exercer aucune autre activité rémunérée. La seconde 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. L'al. 1, 2ème phrase prescrit en outre que le préposé ne peut pas non plus être membre de la direction, de l'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.

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.

8.1.7.4 Art. 40 Surveillance

L'al. 1 pose le principe selon lequel le préposé est l'autorité compétente pour surveiller l'application des dispositions fédérales de protection des données et pour veiller à leur respect. Sa surveillance s'exerce d'une part sur les personnes privées et d'autre part sur les organes fédéraux de manière indépendante et impartiale.

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 (OFSP) par rapport aux assurances maladies, de l'Autorité fédérale de surveillance sur les marchés financiers (FINMA) concernant les banques ou d'autres prestataires financiers ou encore de l'Office fédéral de la communication (OFCOM) par rapport à la commission fédérale de la communication (Comcom). La notion de « 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. 2 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. 41 AP-LPD contre la même partie, l'al. 3 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. 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.

8.1.7.5 Art. 41 Enquête

Tandis que l'art. 27 LPD prescrit que le préposé est chargé de surveiller les traitements de données effectués par les organes fédéraux, l'art. 29, al. 1, LPD dispose que ladite autorité ouvre une enquête à l'encontre d'une personne privée d'office ou à la demande d'un tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (let. a), lorsque des fichiers doivent être enregistrés en vertu de l'art. 11a LPD (let. b) ou lorsqu'il existe un devoir d'information en vertu de l'art. 6, al. 3, LPD (let. c). 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. Il y a dès lors lieu de supprimer les cas énumérés à l'art. 30, al. 1, LPD AP-LPD.

Al. 1 : Ouverture de l'enquête

En vertu de l'art. 41, al. 1, le préposé peut ouvrir une enquête dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données, que ce soit à l'encontre d'un organe fédéral ou d'une personne privée. Il peut ouvrir une enquête d'office ou sur dénonciation. Le dénonciateur peut être un tiers ou la personne concernée. Celui-ci n'a toutefois pas qualité de partie à la procédure

(voir art. 44, al. 2 a contrario). Par contre, si la personne concernée est l'auteur de la dénonciation, le préposé est tenu de l'informer de la suite donnée à sa dénonciation (al. 5).

L'art. 41 laisse une certaine marge de manœuvre au préposé puisque cette disposition ne l'oblige pas à ouvrir une enquête dès qu'il constate la présence de tels indices mais lui donne la faculté de le faire. Il relève par conséquent de la compétence de celui-ci de déterminer l'opportunité d'une telle procédure. Il peut par exemple renoncer à ouvrir une enquête s'il considère que la fourniture de conseils au responsable du traitement concerné peut constituer une mesure suffisante pour remédier à une situation problématique. Par contre, le préposé peut être amené à ouvrir une procédure lorsque par exemple des traitements touchent un grand nombre de personnes et présentent par conséquent un intérêt pour la société en général. En d'autres termes, le préposé intervient lorsqu'il juge qu'il existe un intérêt public suffisant pour ouvrir une enquête mais non pour intervenir en principe dans une affaire qui touche la sphère privée d'un individu. Dans cette seconde hypothèse, la personne concernée doit agir contre une personne privée par la voie civile ou recourir contre la décision de l'organe fédéral devant l'autorité de recours compétente, comme c'est du reste le cas aujourd'hui.

Al. 2 : Devoirs de collaboration

L'al. 2 règle le devoir de collaboration de la personne privée et de l'organe fédéral. 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 confidentialité des informations fournies est garantie puisque le préposé est soumis au secret de fonction au sens de l'art. 22 LPers (art. 37, al. 2, AP-LPD)[109]. L'art. 41, al. 2 correspond aux art. 27, al. 3 et 29, al. 2, LPD. L'art. 50, al. 2, let. c, de l'AP-LPD prévoit une sanction pénale à l'encontre de la personne privée qui violerait son devoir de collaboration, ce que ne fait pas le droit en vigueur.

Al. 3 : Mesures d'investigations

Dans le cadre de son enquête, le préposé peut ordonner certaines mesures d'investigations à l'encontre de la personne privée ou de l'organe fédéral. Cette disposition correspond aux exigences de l'art. 12bis par. 2 let. a du 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 pour les Etats membres une réglementation analogue à son art. 58 par. 1 let. e et f.

Les mesures d'investigation ne respectent le principe de proportionnalité que si les conditions de l'al. 3 sont respectées, soit si la personne privée ou l'organe fédéral ne respecte pas son obligation de collaborer et si toutes les tentatives faites par le préposé pour obtenir les renseignements et les documents nécessaires sont restées vaines. Le préposé peut dans ce cas inspecter sans préavis les locaux de la personne privée ou de l'organe fédéral faisant l'objet d'une surveillance (let. a) et exiger l'accès à toutes les données et informations nécessaires (let. b). Pour l'exécution des mesures de contrôle, le préposé peut requérir l'entraide administrative des autorités fédérales et cantonales (art. 46 AP-LPD). Ces mesures ne peuvent être ordonnées que si une enquête est ouverte.

Al. 4 : Vérification en dehors d'une procédure d'enquête

L'al. 4 précise qu'en dehors d'une procédure d'enquête le préposé est habilité à vérifier si une personne privée ou un organe fédéral respecte les dispositions fédérales de protection des données. Il s'agit par exemple d'obtenir certaines informations du responsable du traitement pour vérifier une situation dont il a connaissance. Dans le cadre de cette vérification, le préposé peut conseiller le responsable du traitement. Si, sur la base des vérifications effectuées, des indices font penser qu'un traitement pourrait être contraire à des prescriptions de protection des données, le préposé ouvre une enquête conformément à l'al. 1. Les mesures

[109] ATF 1C_41/2016 du 22 mars 2016

de contrôle prévues à l'al. 3 ne peuvent être effectuées que si une procédure d'enquête a été ouverte.

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, respectivement du maintien, de la décision d'adéquation de la Commission européenne en faveur de la Suisse.

8.1.7.6 Art. 42 Mesures provisoires

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. 43 AP-LPD confère des compétences décisionnelles au préposé, l'intervention du Tribunal administratif fédéral pour ordonner des mesures provisoires peut être supprimée.

En vertu de l'al. 1, le préposé est dorénavant habilité à ordonner des mesures provisoires en vue de maintenir une situation existante, de protéger des intérêts juridiques menacés ou de préserver des moyens de preuve. Les cas dans lesquels celui-ci peut ordonner de telles mesures sont élargis par rapport au droit en vigueur : le critère déterminant n'est plus seulement l'existence d'un risque pour la personne concernée de subir un dommage irréparable. Des mesures provisoires peuvent aussi être prises lorsqu'il existe un risque de collusion, par exemple, que certaines preuves disparaissent. Le préposé peut par exemple ordonner à la personne privée ou à l'organe fédéral concerné de suspendre un traitement de données pour la durée de l'enquête ou ordonner un séquestre de matériel. Pour l'exécution des mesures provisoires, le préposé peut faire appel à d'autres autorités fédérales ainsi qu'aux organes de police cantonaux et communaux (al. 2).

Conformément à l'art. 44 al. 3 AP-LPD, les recours formés contre les mesures provisoires ordonnées par le préposé n'ont pas d'effet suspensif.

8.1.7.7 Art. 43 Mesures administratives

L'art. 43 AP-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 dispose notamment du pouvoir de prononcer des amendes administratives (let. i) et d'ordonner la suspension de flux de données à un destinataire situé dans un Etat tiers ou à une organisation internationale (art. 58 par. 2 let. j).

L'art. 43, al. 1, AP-LPD est compatible avec l'art. 12^{bis} par. 2 let. c du P-STE 108 en vertu de laquelle chaque Etat-partie est tenu de conférer à l'autorité de contrôle la compétence de rendre des décisions et d'infliger des sanctions administratives. En revanche, le Conseil fédéral propose de ne pas conférer au préposé le pouvoir d'infliger des sanctions administratives mais lui conférer des compétentes décisionnelles et de renforcer les dispositions pénales (ch. 8.1.8).

En vertu de l'art. 43, al. 1, AP-LPD le préposé peut ordonner à une personne privée ou à un organe fédéral de modifier ou de cesser tout ou partie d'un traitement qui serait contraire à des dispositions de protection des données, ainsi que la destruction des données. L'art. 42, AP-LPD laisse néanmoins une certaine marge de manœuvre au préposé puisque cette disposition ne l'oblige pas à prendre des mesures administratives mais lui donne la faculté de le faire. Avant de prononcer de telles mesures, le préposé peut par exemple conseiller le responsable du traitement concerné afin qu'il remédie à la situation. Si le préposé est amené à prononcer une mesure, il doit respecter le principe de proportionnalité. Le cas échéant, il ordonne la modification et non la cessation du traitement et limite la mesure à la partie du traitement problématique.

L'al. 2 correspond aux exigences de l'art. 12 par. 6 du P-STE 108 qui prescrit que l'autorité de contrôle peut interdire ou suspendre le transfert de données personnelles vers un autre pays.

Le préposé notifie sa décision uniquement aux parties à la procédure d'enquête. Le cas échéant, il informe le public conformément à l'art. 48 AP-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. 44).

Toute personne qui ne respecte pas une décision qui lui a été signifiée par le préposé, est punie d'une amende conformément à l'art. 50, al. 2, let. e, AP-LPD.

8.1.7.8 Art. 44 Procédure

Conformément à l'al. 1, la procédure d'enquête et celle de décision sur les mesures visées aux art. 42 et 43 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. 29ss PA).

L'al. 2 précise que seuls l'organe fédéral et la personne privée contre qui une enquête est ouverte ont qualité de partie à la procédure. Par conséquent, seuls ceux-ci peuvent recourir contre les mesures prononcées contre eux par le préposé (art. 42 et 43). 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. 25 AP-LPD, c'est-à-dire devant le juge civil compétent. Dans le secteur public, la personne concernée doit agir contre l'organe fédéral responsable (art. 34), 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.

Conformément à l'al. 3, les recours formés contre les mesures provisoires ordonnées par le préposé en vertu de l'art. 42 n'ont pas d'effet suspensif.

Quant à l'al. 4, 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.

8.1.7.9 Art. 45 Obligation de dénoncer

L'AP-LPD prévoit une obligation pour le préposé de dénoncer aux autorités pénales compétentes les infractions dont il a eu connaissance dans l'exercice de ses fonctions. Par exemple, lorsqu'il constate qu'une personne privée a commis une infraction au sens des art. 50ss AP-LPD, il doit dénoncer le cas aux autorités de poursuite pénale cantonales compétentes (art. 3 et 104 CP). Cette disposition présente l'avantage, par rapport à l'art. 22a LPers, d'étendre le devoir aux contraventions. L'art. 22a LPers s'applique pour le reste.

L'art. 45 est conforme aux exigences de l'art. 47 par. 5 de la directive (UE) 2016/680 et de l'art. 12bis par. 1 let. d du P-STE 108 qui prévoient en substance que l'autorité de contrôle doit disposer du pouvoir de porter à la connaissance de l'autorité judiciaire compétente des violations des dispositions légales en matière de protection des données. Le règlement (UE) 2016/679 prévoit une réglementation analogue à son art. 58 par. 5.

8.1.7.10 Art. 46 Assistance administrative en Suisse

Cette disposition règle l'entraide 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'exécution de la loi. Il s'agit d'une norme standard d'entraide 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. 45 AP-LPD (let. b), ainsi qu'aux autorités fédérales et aux organes de police cantonaux et communaux pour l'exécution des mesures prévues aux art. 41, al. 3, 42 et 43 AP-LPD (let. c).

Les communications visées aux al. 1 et 2 peuvent être effectuées spontanément ou sur demande.

8.1.7.11 Art. 47 Assistance administrative entre autorités suisses et autorités étrangères

Cette disposition règle l'assistance administrative entre le préposé et les autorités chargées de la protection des données à l'étranger. 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 à l'étranger.

Cette disposition transpose l'art. 50 de la directive (UE) 2016/680. Elle correspond également aux exigences des art. 15 et 16 du P-STE 108. Le règlement (UE) 2016/679 prévoit une réglementation analogue à l'art. 61.

Al. 1 : Requête d'assistance administrative à une autorité étrangère

En vertu de l'al. 1, le préposé est en droit de requérir l'assistance administrative d'une autorité étrangère. Il n'est pas nécessaire qu'une enquête soit ouverte au sens de l'art. 41, al. 1, AP-LPD. Le préposé doit adresser sa requête à son homologue étranger, à savoir une autorité chargée de la protection des données dans son pays. Pour transmettre les données personnelles mentionnées à l'al. 1, le préposé doit en outre s'assurer que les conditions prévues à l'art. 5 AP-LPD sont respectées.

L'al. 1 let. a à g définit les informations que le préposé peut communiquer à l'autorité étrangère afin d'obtenir l'assistance administrative. 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. 4, al. 6 AP-LPD (al. 1, 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 (al. 1, let. c, ch. 2). Ces conditions correspondent aux cas prévus à l'art. 29, al. 2, let. a et b AP-LPD.

Al. 2 : Assistance administrative à une autorité étrangère

L'al. 2 règle l'assistance administrative accordée par la Suisse à une autorité étrangère. La première condition figure dans la phrase introductive de l'al. 2, à savoir que l'autorité requérante est une autorité de contrôle en matière de protection des données dans son pays. L'al. 2 énumère aux let. a à e cinq conditions supplémentaires. Conformément au principe de finalité, l'autorité requérante doit s'engager à ne pas utiliser les informations et les données personnelles transmises à d'autres fins que celles indiquées dans la demande d'assistance administrative (let. a). Le principe de réciprocité doit en outre être garanti entre la Suisse et l'Etat étranger (let. b). L'autorité requérante doit de plus s'engager à garantir le respect du secret de fonction ou le secret professionnel et à ne transmettre les informations obtenues à des tiers qu'avec l'autorisation expresse du préposé (let. c et d). Enfin, elle doit respecter les restrictions d'utilisation exigées par le préposé.

Le préposé peut refuser la demande d'assistance administrative par exemple si les conditions de l'art. 5 AP-LPD ne sont pas respectées ou si un des motifs prévus à l'art. 28, al. 6, AP-LPD s'oppose à la communication des données personnelles.

La communication se fait au cas par cas, en principe rapidement et gratuitement.

La transmission d'informations peut être effectuée spontanément ou sur demande de l'autorité étrangère.

8.1.7.12 Art. 48 Information

L'al. 1 correspond à l'art. 30, al. 1, LPD.

L'al. 2 renforce l'information active du préposé. Celui-ci informe le public de ses contestations et de ses décisions, pour autant toutefois que l'information présente un intérêt général pour le public. La seconde phrase de l'art. 31, 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. 29, al. 3 et 5 AP-LPD). Les conditions de l'art. 29, al. 6, AP-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 du P-STE 108. Le règlement (UE) 2016/679 prévoit une réglementation analogue à l'art. 59.

8.1.7.13 Art. 49 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 let. e du P-STE 108.

Le préposé a en particulier pour tâche d'informer et de conseiller les organes fédéraux et cantonaux et les personnes privées dans le domaine de la protection des données. Cela englobe l'organisation de manifestations à but informatif ainsi que celles 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. b). Il doit également fournir, sur demande, aux personnes concernées des informations sur l'exercice de leurs droits (let. c).

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.

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. En effet, l'AP confère au préposé la compétence d'effectuer des mesures de contrôle (art. 40) et de prendre des mesures provisoires (art. 41). Il n'est donc plus nécessaire que celui-ci s'adresse au Tribunal administratif fédéral pour requérir des mesures provisionnelles.

8.1.8 Dispositions pénales

Le Conseil fédéral a fait le choix de ne pas conférer au préposé le pouvoir d'infliger des sanctions administratives. Il aurait fallu pour ce faire, afin de garantir la légitimité et l'acceptance des décisions ainsi que le respect des droits procéduraux des personnes concernées, modifier l'organisation du préposé, sur le modèle de la Commission fédérale de la concurrence par exemple. En raison des coûts que cela aurait engendrés notamment, il y a été renoncé. Par ailleurs, il est préférable de sanctionner les contrevenants dans le cadre de procédures pénales offrant toutes les garanties du code de procédure pénale. Cette option, qui s'inscrit à contre-courant par rapport à la grande majorité des autorités de contrôle étrangères[110] implique en conséquence un renforcement significatif du volet pénal de la loi. Les sanctions doivent être véritablement dissuasives, comme l'exigent le P-STE 108 (art. 10)[111] et de la directive (UE) 2016/680 (art. 57). Le Conseil fédéral estime par ailleurs qu'un système pénal trop souple pourrait conduire la Suisse à se voir refuser le renouvellement de sa décision d'adéquation par l'Union européenne (art. 45 règlement (UE) 2016/679). Le règlement (UE) 2016/679 (art. 83) prévoit en effet, en complément des mesures administratives (art. 58) ou en lieu et place, des amendes administratives très élevées, et ceci pour la viola-

[110] Les autorités des Etats membres de l'Union européenne peuvent en général infliger elles-mêmes des amendes. Il en va de même de celles de l'Argentine, de Singapour, de la Colombie ou encore de la Turquie.

[111] Voir le ch. 95 et 96 du projet de rapport explicatif du CAHDATA du 2 juin 2016.

tion de nombreux devoirs, y compris en cas de négligence (art. 83). Il est ainsi prévu, notamment, d'augmenter le montant des amendes, à un maximum de 500'000.-. Dans la mesure où les personnes physiques continuent à être pénalement responsables en priorité, le montant de l'amende doit cependant rester dans une limite raisonnable. Il ne ferait par ailleurs aucun sens de la calculer en fonction du chiffre d'affaire, comme c'est le cas pour les sanctions administratives visant en priorité les entreprises. Les personnes morales peuvent être directement poursuivies en application de l'art. 53 AP-LPD et 102 CP (voir le commentaire de l'art. 53 AP-LPD).

8.1.8.1 Art. 50 Violation des obligations de renseigner, de déclarer et de collaborer

L'art. 50 AP-LPD reprend sur le principe l'actuel art. 34 LPD en le complétant pour tenir compte notamment des nouvelles obligations incombant aux responsables du traitement et aux sous-traitants.

Montant de l'amende

Cette disposition prévoit d'augmenter le montant de la contravention, qui est aujourd'hui de 10'000.- en vertu de l'art. 106, al. 1 CP, à 500'000.-. Le Conseil fédéral estime en effet, compte tenu du manque de maîtrise des personnes concernées sur leurs données, du manque de transparence des traitements, et des acteurs économiques toujours plus puissants, qu'il est nécessaire de pouvoir infliger des amendes conséquentes. On trouve des contraventions d'un même montant dans d'autres lois fédérales, comme la loi fédérale du 18 décembre 1998 sur les maisons de jeux (LMJ ; art. 56)[112] ou la loi du 8 novembre 1934 sur les banques et les caisses d'épargne (LB; art. 49)[113]. Relevons encore que le règlement (UE) 2016/679 (art. 83) prévoit la possibilité d'infliger des amendes administratives jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, voir même jusqu'à 20 000 000 EUR, respectivement jusqu'à 4 % du chiffre d'affaires annuel mondial. Cela plaide également pour augmenter le montant de l'amende, car cet élément fera vraisemblablement partie des critères déterminants pour évaluer si la législation suisse offre un niveau de protection adéquat au sens de l'art. 45 du règlement (UE) 2016/679. On pourrait certes imaginer de transformer ces contraventions en délits, ce qui permettrait de les punir d'une peine pécuniaire ou d'une peine privative de liberté de trois ans au plus. Le Conseil fédéral y renonce cependant au vu de la gravité inférieure de ces comportements par rapport à ceux envisagés par l'art. 52 (voir le commentaire y relatif). Il se justifie dès lors de conserver les violations des obligations de renseigner, de déclarer et de collaborer au niveau de la contravention, tout en augmentant significativement les possibilités de sanction. Notons encore que le montant prévu constitue un maximum et que la peine doit être concrètement fixée par le juge en tenant compte de la situation économique du contrevenant (art. 106, al. 3, en relation avec l'art. 47 CP). En outre, en application de l'art. 52 CP, il doit être renoncé à toute poursuite pénale ou condamnation en cas de peu de gravité.

Al. 1

L'al. 1 vise les violations d'obligations de renseigner. La let. a sanctionne la personne privée qui fournit intentionnellement des renseignements inexacts ou incomplets dans le cadre du devoir d'information (art. 13 et 15 AP-LPD), et du droit d'accès (art. 20 AP-LPD). Il reprend en substance le contenu du droit actuel (art. 34, al. 1, let. a LPD) en l'adaptant aux nouvelles dispositions pertinentes.

L'al. 1, let. b sanctionne la personne privée qui, intentionnellement, d'une part n'informe pas la personne concernée conformément à l'art. 13, al. 1 et 5, 15 et 17, al. 2 AP-LPD, et d'autre part ne lui fournit pas les indications prévues à l'art. 13, al. 2, 3 et 4 AP-LPD. L'AP-LPD reprend ici aussi en substance le droit actuel (art. 34, al. 1, let. b LPD), en l'adaptant au nouveau contenu du devoir d'information.

L'al. 1, let. c sanctionne la personne privée qui, intentionnellement, ne communique pas au préposé le résultat de l'analyse d'impact selon l'art. 16, al. 3, AP-LPD. Il s'agit d'un élément

[112] RS **935.52**

[113] RS **952.0**

important pour que le préposé puisse exercer son pouvoir de surveillance, et il se justifie donc d'incriminer sa violation. Le règlement (UE) 2016/679 prévoit des sanctions (art. 83, par. 4, let. a).

Al. 2

L'art. 50, al. 2, let. a punit la personne privée qui ne communique pas les garanties spécifiques, notamment contractuelles (art. 5, al. 3, let. b AP-LPD) ou les règles d'entreprises contraignantes (art. 5, al. 3, let. d, ch. 2 et 6 AP-LPD) au préposé, ou qui ne lui annonce pas qu'elle recourt à des garanties standardisées (art. 5, al. 3, let. c, al. 2 et 6 AP-LPD). L'AP-LPD correspond partiellement à l'actuel art. 34, al. 2, let. a LPD en l'adaptant aux nouveaux devoirs en cas de communication transfrontière. La let. b sanctionne le fait de ne pas communiquer pour approbation au préposé les règles standardisées selon l'art. 5, al. 3, let. c, ch. 1 et les règles d'entreprises contraignantes selon l'art. 5, al. 3, let. d, ch. 1 AP-LPD. Il s'agit d'une nouveauté, dans la mesure où ces obligations ne sont pas prévues dans le droit actuel. Le règlement (UE) 2016/679 prévoit, en cas de violation des règles sur le transfert de données à l'étranger, une amende administrative pouvant s'élever à 20 000 000 EUR ou, dans le cas d'une entreprise, à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent (art. 83, al. 5, let. c).

La let. c correspond à l'actuel art. 34, al. 1, al. 2, let. b LPD, « l'établissement des faits » ayant été remplacé par « l'enquête ».

La let. d sanctionne le non-respect de la nouvelle obligation de communiquer au préposé les violations de la protection des données (art. 17, al. 1 AP-LPD). Le Conseil fédéral estime qu'il s'agit là d'un devoir indispensable au préposé pour exercer son pouvoir de surveillance, dont la violation doit être punissable pénalement. Le règlement (UE) 2016/679 prévoit aussi la possibilité de sanctionner la violation de cette obligation (art. 83, par. 4, let. a).

La let. f punit quant à elle le fait de ne pas se conformer à une décision du préposé. Cette disposition est importante pour garantir que les mesures prises par le préposé soient suivies d'effet. Selon le Conseil fédéral, le recours à l'art. 292 CP n'est à cet égard pas suffisant, en raison du montant trop faible de l'amende. Le règlement (UE) 2016/679 prévoit aussi une possibilité de sanction pour ce comportement (art. 83, al. 4, let. e).

Al. 3

L'al. 3 let. a de l'AP-LPD sanctionne la violation du devoir d'informer les destinataires auxquels des données ont été communiquées de toute rectification, effacement, destruction, violation de la protection des données ainsi que toute limitation du traitement (art. 19, let. b AP-LPD). L'al. 3 let. b punit quant à lui la violation du devoir d'informer le responsable du traitement de toute violation de la protection des données (art. 17, al. 4, AP-LPD). Le règlement (UE) 2016/679 prévoit la possibilité d'infliger une amende administrative pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent (art 83. par. 4, let. a).

Les comportements ci-dessus sont aussi punissables si l'auteur agit par négligence. Dans ce cas l'amende est au maximum de 250'000.-. Le règlement (UE) 2016/679 prévoit aussi ce cas de figure (art. 83 par. 2 let. b).

8.1.8.2 Art. 51 Violation des devoirs de diligence

Cette disposition est nouvelle. Elle découle principalement du fait que l'AP-LPD prévoit toute une série de nouvelles obligations qui ne sont pas couvertes par les dispositions pénales actuelles. Le Conseil fédéral estime qu'une protection efficace de la personnalité et des droits fondamentaux des personnes concernées ne peut se faire que moyennant le respect, par les responsables du traitement et les sous-traitants, de l'ensemble de leurs devoirs. En conséquence, et pour inciter ceux-ci à respecter la loi de manière globale, le Conseil fédéral propose de compléter le catalogue des infractions pénales de la loi. Il convient par ailleurs de souligner que le règlement (UE) 2016/679 prévoit la possibilité de sanctionner de tels comportements (art. 83 par. 4 let. a et 5 let. c) aussi en cas de négligence. Cette disposition, ne s'applique pas aux organes fédéraux vu les mesures disciplinaires existantes.

L'art. 51, al. 1 prévoit une amende jusqu'à 500'000 francs pour les personnes privées qui intentionnellement, violent certains devoirs. Cette peine est motivée par les mêmes raisons que celles évoquées à l'art. 50 (voir le commentaire y relatif).

La let. a punit le fait de communiquer des données à l'étranger malgré l'absence de niveau de protection adéquat et sans que les conditions de l'art. 6 soient remplies.

La let. b punit le fait de confier le traitement de données à un sous-traitant en violation de l'art. 7, al. 1 et 2.

La let. c sanctionne le fait de ne pas prendre les mesures nécessaires pour protéger les données contre tout traitement non autorisé et toute perte (art. 11).

La let. d punit le fait de ne pas procéder à une étude d'impact en violation de l'art. 16 AP-LPD.

La let. e sanctionne le fait de ne pas prendre les mesures appropriées au sens de l'art. 18, AP-LPD.

La let. f punit le fait de ne pas documenter les traitements de données conformément à l'art. 19, let. a AP-LPD.

8.1.8.3 Art. 52 Violation du devoir de discrétion

Cette disposition a pour vocation de compléter la protection du secret professionnel instituée par l'art. 321 CP. Cette dernière disposition est devenue lacunaire en raison de la spécialisation grandissante des activités professionnelles et de la sophistication toujours plus importante des méthodes de traitement de l'information. Elle entend ainsi soumettre au devoir de discrétion certaines activités professionnelles non régies par l'art. 321 CP, mais dont l'exercice rend également la protection de la confidentialité indispensable. Le législateur a préféré cette solution à l'extension du champ d'application de l'art. 321 CP, car il a jugé inopportun d'étendre également le droit de refuser de témoigner généralement prévu par les lois de procédure pour les professions visées par l'art. 321 CP[114].

Depuis l'entrée en vigueur de la LPD, les technologies de l'information et de la communication ont connu des progrès et une croissance sans précédents. Les modes de communication électronique se sont généralisés et constituent désormais les moyens prioritaires, sinon exclusifs, de transmettre et conserver l'information. Les moyens techniques sont tels et leurs coûts si faibles qu'il est aujourd'hui à la portée d'un nombre toujours croissant de personnes de traiter des quantités titanesques de données. Alors que les fichiers d'antan imposaient de véritables limites physiques aux possibilités d'archivage, il est devenu de moins en moins nécessaire de détruire des données électroniques anciennes pour faire de la place aux plus récentes. La pérennité des informations est pratiquement assurée. Enfin, l'évolution technologique est incessante et progresse de manière fulgurante, de sorte que ces phénomènes ne peuvent que s'amplifier à l'avenir. Il en découle un danger pour la protection de la sphère privée et une nécessité correspondante de protection.

Compte tenu de ce qui précède, il est opportun d'étendre le devoir de discrétion à tous les types de données personnelles. Le critère déterminant est qu'elles soient secrètes. Cela correspond à l'art. 321 CP, qui s'attache au caractère secret ou non de l'information, et non à son contenu. Cette extension permet aussi d'éviter que la protection pénale ne soit affaiblie par l'abrogation de la notion de « profil de la personnalité ».

Il paraît au surplus nécessaire d'adapter l'énoncé du comportement punissable afin de mieux tenir compte des réalités décrites ci-dessus. Celles-ci ont en effet notamment pour conséquence de grandement faciliter le traitement de données sensibles et le profilage à des fins purement lucratives. On pense ici en particulier aux commerçants et aux réseaux sociaux actifs sur internet qui vendent et achètent de telles informations dans un but publicitaire. L'al. 1, let. b, a donc pour objectif de prévenir et de sanctionner les atteintes au bien juridique protégé qui sont susceptibles de survenir dans le cadre d'activités conçues et exécutées

[114] Message LPD, FF 1988 II 421, 491 ; NIGGLI MARCEL ALEXANDER/MAEDER STEFAN, in: Maurer-Lambrou/Blechta (éds.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3e éd., Bâle 2014, art. 35 LPD n° 1.

dans une intention lucrative, mais pas forcément dans le cadre d'une profession qui nécessite la connaissance de telles données.

Enfin, force est de constater qu'une peine d'amende ne correspond manifestement plus à la gravité des atteintes possibles en particulier au regard de l'art. 321 CP. Il y a lieu dès lors de corriger ce décalage en instituant désormais un délit passible d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

8.1.8.4 Art. 53 Infractions commises dans une entreprise

Cette disposition reprend la réglementation prévue à l'art. 7 de la loi du 22 mars 1974 sur le droit pénal administratif (DPA)[115], en relevant à 100'000 francs le montant maximal de l'amende au-delà duquel il n'est plus possible de poursuivre la personne morale en lieu et place des personnes physiques. L'art. 102 CP n'est en effet pas applicable aux contraventions. Or, pour les raisons évoquées plus haut, la majorité des infractions à la présente loi doivent constituer des contraventions. Dans la mesure toutefois où il est à craindre qu'elles ne soient principalement commises au sein d'entreprises, il se justifie d'appliquer le régime de l'art. 7 DPA pour éviter de nuire d'emblée à l'efficacité des nouvelles dispositions. Un renvoi exprès est nécessaire, puisque la DPA n'est, à défaut, pas applicable en l'espèce. Pour les délits de l'art. 51, l'art. 102 CP demeure en revanche seul applicable.

8.1.8.5 Art. 54 Droit applicable et procédure

La poursuite et le jugement des infractions incombent comme aujourd'hui aux cantons qui appliquent donc le CPP. L'art. 52 constitue en effet un renvoi ponctuel qui n'a aucune portée quant à la loi de procédure applicable.

8.1.8.6 Art. 55 Prescription de l'action pénale

L'expérience a montré que les enquêtes sont en matière de protection des données souvent compliquées et fastidieuses. Or, en matière de contraventions, l'action pénale se prescrit par trois ans (art. 109 CP). Afin d'éviter que les procédures pénales y relatives soient d'emblée vouées à l'échec dans la plupart des cas, l'AP-LPD propose dès lors d'élever à 5 ans le délai de prescription de l'action pénale.

Il n'y a en revanche pas lieu de déroger au délai de prescription de l'action pénale usuel de dix ans pour les délits de l'art. 52 (art. 97, al. 1, let. c, CP).

8.1.9 Conclusions de traités internationaux

Art. 56

L'art. 56 AP-LPD 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 entre la Confédération suisse et l'Union européenne sur la coopération en matière d'application de leurs droits de la concurrence[116]. 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. On pense ici notamment à un éventuel traité avec les Etats-Unis, qui remplacerait l'actuel « U.S-Swiss safe harbor framework ».

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. 2, qui prévoit que le Conseil fédéral peut prévoir

[115] RS **313.0**

[116] Accord entre la Confédération suisse et l'Union européenne concernant la coopération en matière d'application de leurs droits de la concurrence, conclu le 17 mai 2013, RS 0.251.268.1. Notons que dans ce cas, le Conseil fédéral n'avait pas de délégation de compétence.

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.

8.1.10 Dispositions finales et transitoires

8.1.10.1 Art. 57 Exécution par les cantons

Cette disposition correspond à l'art. 37 LPD. Seuls les renvois aux nouvelles dispositions de l'AP-LPD sont adaptés. Pour le surplus, il y a lieu de se référer aux explications présentées dans le message du Conseil fédéral 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[117].

8.1.10.2 Art. 58 Abrogation et modification d'autres actes

L'abrogation et la modification d'autres actes sont commentées sous ch. 8.2.

8.1.10.3 Art. 59 Dispositions transitoires

Les responsables du traitement et les sous-traitants disposent d'un délai de deux ans dès la date d'entrée en vigueur de la loi pour mettre en œuvre d'une part l'obligation d'effectuer une étude d'impact du traitement (art. 16) et d'autre part pour prendre les mesures visées aux l'art. 18 et 19, let. a AP-LPD pour les traitements en cours d'exécution au moment de l'entrée en vigueur de la loi.

8.2 Commentaires relatif à la modification d'autres lois fédérales

L'abrogation et la modification d'autres lois fédérales sont réglées dans l'annexe AP-LPD[118]. Ces modifications sont une conséquence de l'AP-LPD.

8.2.1 Abrogation de la loi du 19 juin 1992 sur la protection des données

Comme l'AP-LPD est une révision totale de de la LPD, cette dernière doit être abrogée.

8.2.2 Modification de la terminologie dans certaines lois fédérales

En raison de la suppression de la notion de « fichier » dans l'AP-LPD, les lois fédérales spéciales qui recourent à ce terme doivent être adaptées. Par ailleurs, la notion de « maître du fichier » est remplacée.

L'AP-LPD prévoit de remplacer la notion de « profils de la personnalité » par celle de « profilage » qui est une notion plus ciblée et axée sur une action (voir le commentaire de l'art. 3, let. f AP-LPD). Pour des raisons de cohérence, la notion de « profil de la personnalité » doit également être remplacée dans la majorité des lois spéciales. Il suffit la plupart du temps de supprimer purement et simplement la référence au profil de la personnalité. Cette suppression n'a pas de conséquence en pratique : en effet, avec l'AP-LPD, une base légale formelle n'est exigée que si le traitement consiste à analyser ou prédire des caractéristiques essentielles, comme le rendement au travail, la situation économique, la santé, la sphère intime, ou les déplacements, c'est à-dire en cas de profilage. Il ne se justifie par conséquent d'introduire cette notion que dans les cas où l'autorité effectue ce type d'analyse ou de prédiction. La base légale prévue par les lois spéciales concernant le traitement de données sensibles reste en revanche inchangée. Dans un certain de nombre de lois - qui sont com-

---

[117] FF **2003** 1915, 1957

[118] Certaines des ces lois fédérales font actuellement l'objet de révisions séparées. Il s'agit de la loi fédérale du 29 septembre 1952 sur l'acquisition et la perte de la nationalité suisse (RS **141.0** ; FF 2014 5001), de la loi fédérale du 4 octobre 1991 sur les écoles polytechniques fédérales (RS **414.110** ; FF 2016 3203) et de la loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (RS **510.10** ; FF 2016 1877). Les art. 27 et 27d LPers seront modifiés par le projet de loi fédérale sur l'établissement chargé de l'administration des fonds de compensation de l'AVS, de l'AI et du régime des APG (FF 2016 271).

mentées ci-après - la notion de « profils de personnalité » doit toutefois être modifiée en tenant compte de la nouvelle notion de « profilage » introduite l'art. 3, let. h AP-LPD.

8.2.3 Loi fédérale du 16 décembre 2015 sur les étrangers[119]

Art. 101

La notion de « profil de la personnalité » est supprimée. Voir le commentaire du ch. 8.2.1.

Art. 111d, al. 2, let. a et b

Actuellement, la let. a prévoit que le consentement de la personne concernée doit être indubitable et, s'il s'agit de données sensibles, explicite. La notion de « consentement » de la personne concernée doit être définie de manière uniforme en droit fédéral. Il y a lieu par conséquent de modifier la let. a, en renvoyant à l'art. 4, al. 6 AP-LPD. Quant à l'al. 2, let. b, est modifié pour tenir compte de la nouvelle disposition prévue à l'art. 6, al. 1, let. d, AP-LPD.

Art. 111f, 2ème 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. 20, al. 2, let. f AP-LPD.

8.2.4 Loi du 26 juin 1998 sur l'asile[120]

Art. 96, al. 1, art. 99a, al. 2, let. a, art. 100, al. 2 et art. 102, al. 1 et 2

La notion de « profil de la personnalité » est supprimée. Voir le commentaire du ch. 8.2.1.

Art. 99, al. 6, 1ère phrase

La notion de maître du fichier est remplacée par celle de « responsable du traitement ».

Art. 102c, phrase introductive, al. 2, let. a et b

Voir le commentaire de l'art. 111d, al. 2, let. a et b AP-LEtr.

Art. 102e, 2ème phrase

Voir le commentaire de l'art. 111f, 2ème phrase AP-LEtr.

8.2.5 Loi du 17 décembre 2004 sur la transparence[121]

Art. 7, al. 2 et 3

L'actuel art. 7, al. 2 LTrans prévoit que le droit d'accès doit être restreint si l'accès à un document officiel peut porter atteinte à la sphère privée d'un tiers, à moins qu'un intérêt public à la transparence ne soit exceptionnellement jugé prépondérant.

En raison des modifications apportées aux art. 11, al. 1, art. 12, al. 3 et 15, al. 2 LTrans, il est nécessaire de modifier la systématique de l'art. 7, al. 2 LTrans. L'AP prévoit par conséquent la limitation du droit d'accès à l'art. 7, al. 2 AP-LTrans et son exception à l'art. 7, al. 3 AP-LPD. Pour le surplus, ces dispositions sont inchangées par rapport au droit en vigueur.

Art. 11, al. 1

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.

---

119 RS **142.31**

120 RS **142.31**

121 RS **152.3**

Vu le nouveau champ d'application de l'AP-LPD, il est nécessaire 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. 3, AP-LTrans. En vertu de la modification apportée à l'al. 1, l'autorité doit dorénavant consulter le tiers concerné lorsqu'elle envisage d'accorder l'accès à un document contenant des données personnelles le concernant ou lorsqu'elle envisage d'appliquer l'art. 7, al. 3 AP-LTrans.

Art. 12, al. 3

Vu la modification apportée aux art. 7, al. 3 et art. 11, al. 1 AP-LTrans, il est nécessaire de modifier l'art. 12, al. 3 en prévoyant que l'accès à un document officiel contenant des données personnelles ou en vertu de l'art. 7, al. 3, AP-LTrans est différé jusqu'à droit connu.

Art. 15, al. 2, let. c (nouveau)

Pour les motifs exposés ci-dessus, il est nécessaire de compléter l'art. 15, al. 2 par une nouvelle lettre c en vertu de laquelle l'autorité doit rendre une décision si, en dérogation à la recommandation du préposé, elle entend accorder l'accès à un document officiel en vertu de l'art. 7, al. 3, AP-LTrans.

8.2.6 Loi fédérale du 20 décembre 1968 sur la procédure administrative[122]

Art. 71a

L'al. 1 transpose un principe jurisprudentiel développé par le Tribunal fédéral[123] qui considère que lorsqu'une question relative à la protection des données apparaît dans le cadre d'une procédure qui a pour objet d'autres prétentions que celles découlant spécifiquement de la LPD, elle doit être tranchée dans le cadre de la procédure principale et suivre les mêmes voies de droit.

Il découle du principe fixé à l'al. 1 que le préposé n'est pas compétent pour surveiller les traitements de données effectués dans le cadre d'une procédure de recours ou de révision (al. 2).

8.2.7 Code civil

L'abrogation de l'exception prévue à l'art. 2, al. 2, let. d, LPD a pour conséquence qu'il est nécessaire de modifier certaines dispositions fédérales du Code civil relatives à l'état civil, afin de tenir compte d'une part du principe fixé à l'art. 9 CC selon lequel les registres publics font foi des faits qu'ils constatent et dont l'inexactitude n'est pas prouvée, et d'autre part de l'intérêt public à garantir la tenue de tels registres (voir considérant 73 du règlement (UE) 2016/679).

Art. 45a, al. 3, ch. 3 et al. 4

L'art. 45a, al. 3, ch. 3 AP-CC[124] charge le Conseil fédéral de régler, avec le concours des cantons, la surveillance de la banque de données centrale «Infostar ». Il s'agit en particulier de modifier l'art. 83 OEC, en s'inspirant par exemple de la solution prévue à l'art. 55, al. 1, de l'ordonnance N-SIS du 8 mars 2013[125] 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 d'Infostar, 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).

En vertu de l'art. 45a, al. 4, AP-CC, le Conseil fédéral peut en outre régler les droits des personnes concernées en adoptant une réglementation spéciale qui déroge tout ou partie à l'art.

---

122 RS **172.021**

123 ATF 128 II 311, considérant 8.4

124 L'art. 45a CC fait actuellement l'objet d'une révision (voir message du Conseil fédéral du 16 avril 2014concernant la modification du code civil (Enregistrement de l'état civil et registre foncier), FF **2014** 3395)

125 RS **362.0**

32, al. 1 à 3, AP-LPD. Il s'agit d'une délégation législative facultative. Le Conseil fédéral peut recourir à cette faculté s'il arrive à la conclusion que l'adoption de dispositions spéciales est nécessaire au regard de la finalité poursuivie par le registre central, tout en tenant compte des exigences de la future convention STE 108 dans l'hypothèse où la Suisse accepte le protocole d'amendement de cet acte.

8.2.8 Loi fédérale du 24 mars 2000 sur le traitement des données personnelles au Département fédéral des affaires étrangères[126]

Art. 1, 1e phrase et art. 2, al. 2, 1e phrase

Afin d'apprécier les possibilités d'employer à l'étranger une personne accompagnée de membres de sa famille et d'évaluer les risques que comporte leur situation personnelle, l'art. 3 habilite les services du personnel du DFAE à traiter des données relatives aux membres de la famille de l'employé. Ces dispositions doivent donc être reformulées afin que le traitement de données sensibles et le profilage soient autorisés.

8.2.9 Code de procédure civile[127]

8.2.9.1 For

L'art. 20 CPC règle dorénavant le for pour les actions civiles en matière de protection des données. Il s'agit notamment des actions en exécution du droit de consultation et à l'effacement selon l'art. 12 AP-LPD, l'action en exécution du droit d'accès de l'art. 20 AP-LPD et pour les actions selon l'art. 25 AP-LPD.

8.2.9.2 Suppression des frais de justice

L'évaluation de la loi sur la protection des données a montré que les personnes concernées sont peu enclines à faire valoir leurs droits, notamment contre des privés, par peur avant tout du coût des procédures[128]. L'efficacité de la loi sur la protection des données dans le secteur privé s'en trouve considérablement réduite. Cette retenue a par ailleurs empêché le développement, dans le domaine de la protection des données, d'une jurisprudence différenciée, qui concrétise les normes et garantisse une certaine sécurité juridique.

Afin de simplifier la mise en œuvre procédurale des droits des personnes concernées, l'AP-LPD prévoit, comme mesure principale, de supprimer les frais de justice pour les actions civiles en matière de protection des données. Cette mesure s'applique déjà dans d'autres procédures et domaines (par ex litiges découlant de la loi sur l'égalité ou en matière de droit du travail dont l'enjeu n'excède pas 30'000.-, ou litiges relevant de la loi sur la participation). Il ne faut cependant pas s'attendre à une envolée du nombre d'affaires portées devant les tribunaux, notamment parce que la partie qui succombe devra toujours verser des dépens et assumer ses frais de représentation, et que les 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. Cette obligation est supprimée pour les procédures relevant de la loi sur la protection des données. La charge financière de la partie demanderesse est ainsi réduite.

Cette suppression concerne les actions au sens de l'art. 25 AP-LPD qui sont traitées dans le cadre de la procédure ordinaire. Elle vise à faciliter de telles actions, qui ne sont que rarement intentées. Les personnes qui introduisent une procédure simplifiée au sens de l'art. 243, al. 2, let. d, CPC sont déjà exemptées de l'obligation de fournir des sûretés (voir l'art. 99, al. 3, CPC). Cela ne va pas changer.

---

126 RS **235.2**

127 RS **272**

128 Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 260 s.

Art. 113, al. 2, let. g

Le CPC est complété de manière que, pour les procédures de conciliation menées en vertu de la loi sur la protection des données, qui sont en principe obligatoires aussi bien dans la procédure ordinaire que dans la procédure simplifiée (art. 197 CPC), il n'est pas perçu de frais judiciaires. 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 (voir l'art. 113, al. 2, CPC).

L'exemption des frais judiciaires réduit le risque financier encouru par la personne concernée pour toutes les actions civiles intentées en vertu de la protection des données. Cela est d'autant plus déterminant qu'il n'est en principe pas alloué de dépens en procédure de conciliation (voir l'art. 113, al. 1, 1re phrase, CPC). Le requérant doit en principe prendre à sa charge ses frais d'avocat, à moins de bénéficier de l'assistance judiciaire.

Art. 114, let. f

Le CPC est complété de manière à ce que, dans la procédure au fond, il n'est pas perçu de frais judiciaires pour les litiges relevant de la loi sur la protection des données, comme c'est par exemple le cas pour les litiges relevant de la loi sur l'égalité ou de la loi sur la participation et les litige touchant au droit du travail d'un enjeu s'élevant à 30'000.- 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 (voir les art. 104 ss CPC).

8.2.9.3 Procédure applicable

Art. 243, al. 2, let. d

Les actions selon l'art. 12 AP-LPD sont soumises, comme les actions en exécution du droit d'accès, à la procédure simplifiée. Cette modification est nécessaire dans la mesure où l'art. 12 AP-LPD est nouveau.

8.2.10 Loi fédérale du 18 décembre 1987 sur le droit international privé[129]

Art. 130 al. 3

Cette disposition doit être modifiée dans la mesure où l'AP-LPD supprime la notion de « fichier ».

L'art. 130, al. 3, AP-LDIP prévoit que les actions en exécution du droit du droit d'accès et de consultation dans le cadre d'un traitement de données personnelles peuvent être intentées devant les tribunaux mentionnés à l'art. 129 LPDIP ou devant les tribunaux suisses du lieu où les données personnelles sont traitées. Un droit d'accès qui se rapporte à une activité déterminée, doit ainsi être intenté là où cette activité a lieu, et non dans

Ein Auskunftsrecht, das sich auf eine bestimmte Tätigkeit bezieht, muss dort geltend gemacht werden, wo diese bestimmte Tätigkeit stattfindet, und nicht an irgendeinem anderen Ort, an dem die Daten sonst noch von jemandem bearbeitet werden.

8.2.11 Code pénal

Art. 179novies

Cette disposition réprime la soustraction de données personnelles, qui ne sont pas accessibles à tout un chacun. Il se justifie, compte tenu des nombreux développements technologiques, d'étendre le champ d'application de la disposition à tous les types de données personnelles, comme c'est le cas pour le devoir de discrétion de l'art. 52 AP-LPD (ch. 8.1.8.3). Il faut en particulier souligner que le profilage (art. 3, let. f AP-LPD), qui entraîne un danger particulier pour la personne concernée, résulte de l'analyse de données personnelles mais aussi d'autres données. Or, ces dernières deviennent, à l'issue du profilage, des données

[129] RS **291**

personnelles. Il est en conséquence justifié d'englober dans la protection de l'art. 170^{novies} tous les types de données personnelles.

La disposition fait en outre l'objet d'une modification terminologique. Les termes de « qui ne sont pas librement accessibles » sont remplacés par « qui ne sont pas accessibles à tout un chacun ».

Art.179^{decies}

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.

Dans un contexte juridique, 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 sa 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[130]. 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 nous retient 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 sanctionnera aussi l'auteur qui aura par exemple commandé par écrit une marchandise ou qui aura pris des renseignements auprès d'une personne âgée pour se faire passer ensuite au téléphone pour un de ses petits-enfants. La disposition ne s'appliquera 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[131].

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[132] 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 (com-

130 Art. 173 ss CP

131 Pour un élément constitutif d'infraction identique dans le cadre d'un abus d'autorité, voir HEIMGARTNER STEFAN, in: Niggli/Wiprächtiger (édit.), Basler Kommentar, Strafrecht II, 3e édition, Bâle 2013, ad art. 312 CP n° 23.

132 Art. 179^{novies} CP

mise 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, puni 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 ex. commis dans le cadre d'une instruction policière ou d'une enquête pénale) demeurent licites en vertu de l'art. 14 CP.

8.2.12 Loi fédérale du 22 mars 1974 sur le droit pénal administratif[133]

La 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).Vu la nouvelle teneur de l'art. 2, al. 2, let. c, AP-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

Cette disposition règle la transparence de la collecte de données personnelles. Il s'agit d'une disposition spéciale qui prime les 13 et 14 AP-LPD. Elle correspond à la réglementation prévue à l'art. 95 CPP.

Art. 18b

Voir par analogie le commentaire de l'art. 349g, al. 4, AP-CP (ch. 8.3.1.7).

Art. 18c

Cette norme régit la divulgation 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

Cette disposition règle le droit aux renseignements dans le cadre d'une procédure pendante. Il s'agit d'une disposition spéciale qui prime les art. 20 et 21 AP-LPD. Elle correspond à la réglementation prévue à l'art. 97 CPP.

Art. 18e

Cette disposition règle l'exactitude des données. Elle correspond à la réglementation prévue à l'art. 98 CPP. Il s'agit d'une disposition spéciale qui prime l'art. 4, al. 5, AP-LPD ainsi que l'art. 34, al. 2, AP-LPD. En ce qui concerne l'al. 2, il convient de se référer au commentaire de l'art. 98, al. 2, AP-CPP (voir ch. 8.3.2).

Art. 18f

L'al. 1 transpose un principe jurisprudentiel développé par le Tribunal fédéral[134] qui considère que lorsqu'une question relative à la protection des données apparaît dans le cadre d'une procédure qui a pour objet d'autres prétentions que celles découlant spécifiquement de la LPD, elle doit être tranchée dans le cadre de la procédure principale et suivre les mêmes voies de droit que cette procédure.

Il découle du principe fixé à l'al. 1 que le préposé n'est pas compétent pour surveiller les traitements de données effectués par l'autorité administrative fédérale dans le cadre d'une procédure pénale administrative tant que la décision finale n'est pas exécutoire (al. 2). Cette

[133] RS **313.0**

[134] ATF 128 II 311, consid. 8.4

précision est nécessaire au motif que les autorités administratives fédérales ne sont pas en règle générale des autorités judiciaires indépendantes au sens de l'art. 2, al. 2, let. c AP-LPD. La surveillance du respect des principes de protection des données dans le cadre d'une procédure pendante est garantie par le contrôle indépendant exercé par l'autorité judiciaire de recours, ce qui constitue un système de surveillance équivalent à celui du préposé.

8.2.13 Procédure pénale militaire du 23 mars 1979 (PPM)[135]

La justice militaire est une autorité judiciaire indépendante (art. 1 PPM). Elle tombe sous le coup de l'exception de l'art. 2, al. 2, let. c AP-LPD. La PPM 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

Cette disposition règle la transparence de la collecte des données personnelles. Il s'agit d'une disposition spéciale qui prime les art. 13 et 14 AP-LPD. Elle correspond à la réglementation prévue à l'art. 95 CPP.

Art. 25b

Voir par analogie le commentaire de l'art. 349g, al. 4, AP-CP (ch. 8.3.1.7).

Art. 25c

Cette disposition règle la divulgation et l'utilisation de données personnelles dans le cadre d'une procédure pendante. Elle correspond à l'art. 96 CPP.

Art. 25d

Cette disposition règle le droit aux renseignements dans le cadre d'une procédure pendante. Il s'agit d'une disposition spéciale qui prime les art. 20 et 21 AP-LPD. Elle correspond à l'art. 97 CPP.

Art. 25e

Cette disposition règle l'exactitude des données. Elle correspond à l'art. 98 CPP. Il s'agit d'une disposition spéciale qui prime l'art. 4 al. 5, AP-LPD ainsi que l'art. 34, al. 2, AP-LPD. Pour le surplus, il convient de se référer au commentaire de l'art. 349g, al. 2 AP-CP (ch. 8.3.1.7).

8.2.14 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération[136]

Art. 5, titre, 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 régie à l'art. 7 AP-LPD. L'art. 5, al. 2 LSIP est donc superflu. Le titre de cette disposition doit être adapté en conséquence.

8.2.15 Loi du 9 octobre 1992 sur la statistique fédérale[137]

Art. 14a, al. 1, 1ère et 2e phrase

L'art. 14a règle l'appariement de données. Selon les cas il peut aussi s'agir de profilage. Il convient donc de compléter l'al. 1 et de prévoir que l'office peut faire du profilage pour exécuter ses tâches en matière de statistique. La deuxième phrase de l'al. 1 prescrit que si des

135 RS **321.0**

136 RS **361**

137 RS **431.01**

données sensibles sont appariées ou si l'appariement de données permet d'établir des profils de la personnalité, les données appariées doivent être effacées une fois les travaux statistiques d'exploitation terminés. Il y a lieu de modifier cette disposition en prévoyant que si les données doivent être effacées une fois les travaux statistiques d'exploitation terminés.

8.2.16 Loi du 3 février 1995 sur l'armée

Art. 31, al. 2

Compte tenu 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 « profilage ».

Art. 99, al. 2

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 « profilage ».

Art. 100, al. 2

En raison de la nature des tâches du service de sécurité militaire, il y a lieu de remplacer la notion de « profil de la personnalité » par celle de « profilage ».

8.2.17 Loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée[138]

Art. 1, al. 1, phrase introductive et 11, al. 2, phrase introductive

En raison de la nature des tâches de l'armée et de l'administration militaire, il y a lieu de remplacer la notion de « profil de la personnalité » par celle de « profilage ».

8.2.18 Loi fédérale du 20 juin 1997 sur les armes[139]

Art. 32e, al. 2, let. a et b

Voir le commentaire de l'art. 111d, al. 2, let. a et b AP-LEtr.

Art. 32g, 2ème phrase

Voir le commentaire de l'art. 111f, 2ème phrase AP-LEtr.

8.2.19 Loi fédérale du 4 octobre 2002 sur la protection de la population et sur la protection civile[140]

Art. 72, al. 1 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[141]. Il y a lieu dès lors de modifier cette disposition en prévoyant que celle-ci est habilitée à effectuer des profilages au sens de l'art. 3, let. h, AP-LPD.

8.2.20 Loi fédérale du 21 décembre 1948 sur l'aviation[142]

Art. 107a, al. 2, 4 et 5

Le droit en vigueur prévoit que l'autorité fédérale compétente est habilitée à évaluer l'aptitude du personnel aéronautique civil. Il convient par conséquent de modifier la phrase introductive de l'al. 2 afin de prévoir la compétence de faire du profilage.

---

138 RS **510.91**

139 RS 514.54

140 RS **520.1**

141 L'art. 72 fait l'objet d'une révision qui devrait entrer en vigueur le 1er janvier 2017 (voir FF **2014** 6673).

142 RS **748.0**

En revanche, à l'al. 5, la notion de « profils de la personnalité » est simplement tracée. Dans la mesure où les données qui résultent d'un profilage constituent des données personnelles, la base légale pour leur communication est donnée.

8.2.21 Loi fédérale du 3 octobre 1951 sur les stupéfiants[143]

Art. 3f, al. 1

La notion de « profil de la personnalité » est supprimée. Voir le commentaire du ch. 8.2.2.

Art. 18c, 2ème phrase

Voir le commentaire de l'art. 111f, 2ème phrase AP-LEtr.

8.3 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.

8.3.1 Code pénal

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 applicables aux échanges de données effectués dans le domaine de la coopération policière.

8.3.1.1 Art. 349a

Cette disposition pose le principe selon lequel les traitements de données effectués dans le domaine de l'entraide policière sont régis par les dispositions fédérales et cantonales de protection des données, sous réserve des dispositions spéciales prévues aux art. 349bss AP-CP. Ces dispositions s'appliquent donc également aux autorités cantonales, à moins que la norme ne vise expressément une autorité fédérale. 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 fédérale 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.

8.3.1.2 Art. 349b

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. Pour mettre en œuvre les exigences de la directive (UE) 2016/680, l'art. 349b déroge à l'art. 29 AP-LPD. A défaut de base légale, les autorités fédérales sont ainsi en droit de communiquer des données uniquement dans les cas prévus à l'art. 349b, let. a et b. Ces dispositions correspondent aux lettres c et d de l'art. 29, al. 2, AP-LPD. Par contre, les autorités fédérales compétentes ne peuvent pas se prévaloir des cas de communication prévus à l'art. 29, al. 2, let. a, b et e AP-LPD, car ils ne sont pas compatibles avec les exigences des art. 8 et 10 de la directive (UE) 2016/680.

8.3.1.3 Art. 349c

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. 349c 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.

[143] RS **812.121**

L'adoption de nouvelles restrictions légales reste possible, pour autant que le principe d'égalité soit respecté.

8.3.1.4 Art. 349d

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 transférées à un Etat tiers ou à un organisme international que si certaines conditions cumulatives sont remplies.

L'art. 349d s'inspire de la systématique et du contenu des art. 5 et 6 AP-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 personnalité 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 l'al. 2, let. a, la législation d'un Etat tiers assure un « niveau de protection des données adéquat » lorsque la Commission l'a constaté par voie de décision conformément à l'art. 36 de la directive (UE) 2016/680. L'al. 2, let. a se distingue de l'art. 5, al. 2 AP-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. 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.

L'al. 2, let. b et c prévoit 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. a) soit par des garanties spécifiques (let. b). L'al. 2, let. b correspond à la condition prévue à l'art. 5, al. 3, let. a, AP-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, par exemple la convention STE 108 et son protocole additionnel[144]. Quant à l'al. 2, let. c, il correspond à la condition de l'art. 5, al.3, let. b, AP-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 ce dernier fournit des garanties spécifiques, qui assurent une protection adéquate de la personne concernée.

Al. 3

Conformément à l'al. 3, l'autorité fédérale compétente doit communiquer au préposé les catégories de communications de données personnelles qui ont été effectuées conformément

[144] Voir considérant 69 de la directive (UE) 2016/680.

à l'al. 2, let. c. Il ne s'agit pas d'informer cette autorité 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, 2ème phrase, les communications doivent être documentées. Cette documentation permet au préposé de procéder aux vérifications nécessaires et de prononcer le cas échéant une interdiction en vertu de l'art. 43, al. 2, AP-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.

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. Ici, 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. L'autorité fédérale doit communiquer au préposé les communications effectuées en vertu de l'al. 4 (al. 5).*Al. 6*

L'al. 6 réserve les dispositions relatives à l'octroi de la coopération internationale en matière pénale. En effet, le niveau de protection adéquat exigé à l'al. 1 n'est pas l'unique condition à remplir pour qu'une communication de données à un Etat tiers soit licite ; il faut encore que les dispositions légales en matière de coopération internationale soient respectées. Ainsi, des données ne peuvent être transmises à un Etat tiers que si l'autorité destinataire est compétente pour prévenir, constater ou poursuivre une infraction et que cette communication est nécessaire pour l'accomplissement de ses tâches légales. De plus, tout traitement ultérieur des données par l'autorité destinataire doit respecter les règles du principe de spécialité. Si cette dernière envisage de transférer les données à un autre Etat tiers, elle doit obtenir préalablement l'accord de l'autorité compétente qui a procédé au transfert initial.

8.3.1.5 Art. 349e

Cette disposition met en œuvre les exigences de l'art. 35 par. 1 let. c et e ainsi que par. 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. 349e correspond à l'art. 6b 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 ainsi que let. a de l'al. 1). 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. 349d (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).

8.3.1.6 Art. 349f

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 l'autorité peut 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[145].

Selon la définition de l'art. 3 par. 8 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. A l'art. 349f, la notion de « destinataire » est désignée par le terme de « tiers ».

Al. 1

En vertu de l'al. 1, une communication de données personnelles à un tiers établi dans un Etat tiers ne peut être envisagée que si quatre conditions cumulatives sont remplies. Les communications de données en vertu de l'art. 349f 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 (al. 1, let. a) prescrit que la communication doit être prévue par une législation spéciale ou par un accord international. En effet, l'art. 349f ne constitue pas une base légale en soi pour communiquer des données personnelles. Il faut encore que les dispositions légales en matière de coopération internationale soient respectées.

L'al. 1, let. b prescrit quant à lui que la communication doit être indispensable à l'accomplissement d'une tâche légale de l'autorité compétente, c'est-à-dire des tâches dans le domaine de la prévention, de la constatation ou de la poursuite d'une infraction. La communication doit en outre être indispensable. Le recours à l'art. 349f ne doit dès lors pas constituer une solution de facilité pour l'autorité compétente. La communication est indispensable uniquement 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 (al. 1, let. c). 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 tiers avec l'interdiction expresse de les utiliser pour d'autres finalités que celles qui ont été fixées par l'autorité. 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 (considérant 73 de la directive (UE) 2016/680).

[145] Considérant 73 de la directive (UE) 2016/680

Al. 4

L'al. 4 dispose que l'autorité fédérale compétente doit également informer immédiatement le préposé de toute communication de donnés effectuée en vertu de l'art. 349f. Contrairement à l'obligation prévue à l'art. 349d, 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. 4). Cette documentation permet au préposé de procéder aux vérifications nécessaires et de prononcer le cas échéant une interdiction en vertu de l'art. 43 AP-LPD.

8.3.1.7 Art. 349g

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. Elle doit prendre, dans la mesure du possible, les mesures nécessaires pour éviter une confusion entre les différentes catégories de personnes concernées avant de communiquer des données les concernant à un destinataire. 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.

Quant à l'al. 4, let. b, il 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. Selon le considérant 30 de cet acte, cette disposition est motivée par le fait que cette seconde catégorie comprend des données fondées sur des perceptions subjectives de personnes physiques et qui ne sont pas toujours vérifiables et que par conséquent le principe d'exactitude ne devrait pas s'appliquer à l'exactitude de la déclaration elle-même, mais simplement au fait qu'une déclaration déterminée a été faite[146].

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.

8.3.1.8 Art. 349h

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 en cas de restriction des droits de

[146] Considérant 30 de la directive (UE) 2016/680

la personne concernée de demander l'accès à ses données, la limitation du traitement ou la rectification ou l'effacement des données la concernant. La réglementation de l'art. 349h s'inspire de la solution prévue à l'art. 8 de la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)[147] avec les modifications qui y sont apportées par le présent projet (voir ci-après ch. 8.3.6).

L'al. 1 prescrit que la personne concernée peut, dans les cas prévus aux let. a à d, 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. 349h 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. 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, soit selon le libellé défini à l'al. 3. La communication n'est pas susceptible de recours (al. 3 et 5).

Si le préposé décide d'ouvrir une enquête contre l'autorité fédérale, la personne concernée n'est pas partie à la procédure (art. 44 al. 2 AP-LPD a contrario). Elle ne peut donc pas recourir contre les éventuelles mesures administratives prononcées par le préposé (art. 43 AP-LPD).

8.3.1.9 Art. 349i

Cette disposition met en œuvre l'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. 41, al. 1, AP-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. 44, al. 2, AP-LPD a contrario). 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. 349i, al. 1, la personne concernée peut dès lors demander au préposé d'ouvrir une enquête. Pour que sa requête soit recevable, celle-ci 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. 349d AP-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 (voir commentaire de l'art. 349h, al. 2, AP-CP). Le cas échéant, le préposé peut prendre des mesures provisoires ou administratives contre l'autorité fédérale concernée (art. 42 et 43 AP-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.

8.3.1.10 Art. 355a, al. 1 et 4

Vu que l'AP-LPD supprime la notion de « profils de personnalité », ce terme doit également être supprimé de l'al. 1 (voir commentaire ch. 8.2.2).

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. 349c). Selon le considérant 71 de la directive (UE) 2016/680, les accords de coopération conclus entre

[147] RS **361**

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.

8.3.1.11 Art. 355f et art. 355g

Ces dispositions avaient été introduites lors de la reprise par la Suisse de la décision 2008/977/JAI.

L'art. 355f CP règle la communication de données provenant d'un Etat Schengen à un Eta 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 réglée dans l'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. 355g peut être supprimé.

8.3.2 Code de procédure pénale[148]

Art. 95a

Cette disposition met en œuvre les exigences des art. 6 et 7 par. 1 de la directive (UE) 2016/680. La let. a tient compte de la problématique liée au changement de catégorie des personnes concernées qui peut intervenir avec l'avancement de la procédure. La distinction entre les données personnelles fondées sur des faits de celles fondées sur des appréciations personnelles s'effectue, en ce qui concerne les autorités de jugement, dans les considérants du jugement dûment motivé. Pour le surplus, il convient de se référer par analogie au commentaire de l'art. 349g, al. 3, AP-CP (ch. 8.3.1.7).

Art. 98, al. 2

L'art. 98 règle le principe d'exactitude. Il s'agit d'une disposition spéciale qui prime l'art. 4 al. 5, AP-LPD ainsi que l'art. 34, al. 2, AP-LPD. En ce qui concerne la modification apportée à l'al. 2, il convient de se référer au commentaire de l'art. 349g, al. 2 AP-CP (ch. 8.3.1.7).

8.3.3 Loi fédérale du 24 mars 1981 sur l'entraide pénale internationale[149]

Le présent projet introduit dans l'EIMP une nouvelle section 1b relative à la protection des données qui s'inspire en partie de la solution retenue par le législateur fédéral aux art. 95 et suivants du CPP. Ces dispositions mettent également en œuvre certaines exigences de la directive (UE) 2016/680. Il s'agit de dispositions spéciales de protection des données qui priment les principes généraux de l'AP-LPD, aussi longtemps qu'une procédure d'entraide judicaire est pendante.

8.3.3.1 Art. 11b

L'art. 11b règle le devoir d'information de l'autorité lorsqu'elle traite des données personnelles dans le cadre d'une procédure d'entraide ouverte à la demande d'un Etat étranger. Cette norme constitue une disposition spéciale de protection des données qui prime les art. 13 et 14 AP-LPD. L'art. 11b s'applique également aux autorités cantonales qui collaborent à une procédure d'entraide ou qui sont chargées d'exécuter une demande d'entraide, telle qu'une demande d'extradition. 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 vertu de l'al. 1, l'autorité compétente, c'est-à-dire l'autorité qui est chargée de statuer sur la demande de coopération de l'Etat étranger (art. 1, al. 1, EIMP), est tenue d'informer la personne visée par une telle demande. Il s'agit de toute personne poursuivie ou condamnée

148 RS **312.0**

149 RS **351.1**

pénalement contre laquelle l'Etat étranger requiert la coopération de la Suisse pour obtenir l'extradition de la personne concernée, lui déléguer la poursuite et la répression d'une infraction commise par celle-ci ou exécuter une décision pénale étrangère prononcée à son encontre (art. 1, al. 1, let. a, c et d EIMP). L'autorité doit également informer les ayants droit à une procédure d'entraide en faveur d'une procédure pénale étrangère, tels qu'ils sont définis à l'art. 80b EIMP.

Le devoir d'information de l'autorité n'est toutefois pas absolu. Ainsi, celle-ci est déliée de son obligation si un intérêt public ou privé prépondérant s'oppose à l'information de la personne concernée. 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 informer la personne concernée si elle arrive à la conclusion qu'un intérêt privé ou public prime l'intérêt de la personne concernée à être informée.

L'al. 2 énumère les cas dans lesquels l'intérêt public l'emporte. Selon cette disposition, l'intérêt public est jugé prépondérant notamment lorsque l'information de la personne concernée risque de compromettre une enquête, une procédure d'instruction, une procédure judiciaire ou une procédure de coopération internationale en matière pénale, par exemple l'arrestation de la personne poursuivie en vue d'extradition. Il s'agit d'une liste non exhaustive. L'autorité peut donc s'appuyer sur d'autres éléments spécifiques au cas d'espèce.

Les art. 52 et 80b EIMP s'appliquent pour le surplus.

8.3.3.2 Art. 11c

Cette disposition règle le droit aux renseignements dans le cadre d'une procédure pendante. Elle correspond à l'art. 97 CPP. Il s'agit d'une disposition spéciale qui prime les art. 20 et 21 AP-LPD. Seule la personne visée par une demande de coopération en matière pénale peut, dans les limites de son droit de consulter le dossier, obtenir les données personnelles qui la concernent.

Les art. 52 et 80b EIMP s'appliquent pour le surplus.

8.3.3.3 Art. 11d

Cette disposition introduit une restriction au droit d'accès applicable aux 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. 8.3.6). L'art. 11 d 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 la licéité d'un traitement de données la concernant en cas de restriction de son droit d'accès.

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, 3, 4, 5 et 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, l'AP 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. 11d 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. En vertu de l'al. 3, le préposé effectue la vérification demandée. Celui-ci 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, 4, 5 et 6 coïncident avec les dispositions correspondantes de l'art. 349h AP-CP.

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.

8.3.3.4 Art. 11e

Cette disposition règle l'égalité de traitement entre les autorités Schengen et les autorités nationales en matière de protection des données. Pour le surplus, voir le commentaire de l'art. 349c AP-CP (ch. 8.3.1.3).

8.3.3.5 Art. 11f

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. 349d AP-CP. Toutefois, contrairement à l'art. 349d, al. 3 AP-CP, l'art. 11f ne prévoit pas une obligation pour l'autorité compétente de communiquer au préposé les catégories de communications de données personnelles effectuées conformément à l'art. 11f, al. 2, let. c. Cette différence se justifie par la nécessité d'introduire à l'art. 11i, al. 2 la règle selon laquelle le préposé n'est pas compétent pour surveiller les traitements de données effectués dans le cadre d'une procédure d'entraide judiciaire en cours (voir ci-dessous le commentaire de l'art. 11i). Pour le surplus, il y a lieu de se référer au commentaire relatif à l'art. 349d AP-CP (voir ch. 8.3.1.4).

8.3.3.6 Art. 11g

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. 349e AP-CP. Toutefois, contrairement à l'art. 349e, al. 1, let. a, AP-CP, l'art. 11g, 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 au commentaire relatif à l'art. 349e AP-CP (voir commentaire ci-dessus ch. 8.3.1.5).

8.3.3.7 Art. 11h

Cette disposition règle l'exactitude des données. Il s'agit d'une disposition spéciale qui prime l'art. 4 al. 5, AP-LPD ainsi que l'art. 34, al. 2, AP-LPD. Pour le surplus, cette norme correspond à l'art. 349g AP-CP (voir commentaire ci-dessus ch. 8.3.1.7).

8.3.3.8 Art. 11i

Cette disposition règle les prétentions en matière de protection des données des personnes visées par une demande de coopération en matière pénale dans le cadre d'une procédure d'entraide pendante. Elle correspond à la solution prévue à l'art. 18g AP-DPA, sous réserve que l'al. 2 exclut expressément l'application des art. 20 et 21 AP-LPD relatif au droit d'accès de la personne concernée, l'art. 30 AP-LPD qui prévoit un droit de s'opposer à une commu-

nication de données personnes et l'art. 34 AP-LPD relatif aux prétentions en cas de traitements de données illicites par un organe fédéral. Pour le surplus, il convient de se référer au commentaire de l'art. 18g AP-DPA (voir ch. 8.2.12).

8.3.4 Loi fédérale du 3 octobre 1975 relative au traité conclu avec les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[150]

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* à 11d et 11*g* à 11*i* AP-EIMP (art. 9a). L'art. 11e AP-EIMP ne s'applique pas puisqu'il instaure une égalité de traitement uniquement entre autorités Schengen et autorités pénales suisses en matière de protection des données. A l'instar de l'art. 7, al. 3 de la loi relative au traité conclu avec les Etats-Unis d'Amérique, l'art. 9a réserve les dispositions du traité du 25 mai 1973 entre la Confédération suisse et les Etats-Unis d'Amérique sur l'entraide judiciaire en matière pénale[151].

8.3.5 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[152]

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. 349a à 349i AP-CP.

8.3.6 Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération

Art. 7, al. 2

L'al. 2 réserve également le nouvel art. 8bis.

Art. 8, al. 2, 3, 4, 5, 6, et 8

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. 41 AP-LPD et à prononcer, le cas échéant, des mesures administratives en vertu des art. 42 et 43.

L'al. 2 subit une modification rédactionnelle.

La seconde alternative de la 2ème phrase de l'al. 3 est modifiée en ce sens que le préposé ne doit plus indiquer à la personne concernée « (…) qu'il a adressé une recommandation à fedpol d'y remédier en vertu de l'art. 27 LPD » mais « qu'il a ouvert une enquête conformément à l'art. 41 LPD ». Vu que les art. 42 et 43 AP-LPD confèrent des compétences décisionnelles au préposé, l'intervention du Tribunal administratif fédéral telle qu'elle est prévue à la dernière phrase de l'al. 3 ainsi qu'à l'al. 5 peut être supprimée.

L'al. 4 peut être abrogé. Le renvoi à l'art. 41 AP-LPD est suffisant.

L'enquête du préposé peut aboutir à une décision (art. 43 AP-LPD) contre laquelle fedpol peut recourir (al. 5).

L'al. 6 subit des modifications rédactionnelles. L'al. 8 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

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.

---

150 RS **351.93**

151 RS **0.351.933.6**

152 RS **360**

Cette norme correspond à l'art. 11e AP-EIMP. Il convient dès lors de se référer au commentaire y relatif (ch. 8.3.3).

8.3.7 Loi fédérale du 12 juin 2009 sur les systèmes d'information Schengen

Art. 2, al. 3

Les art. 6a à 6c LEIS 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 de supprimer ces dispositions et de prévoir un renvoi aux art. 349a à 349i AP-CP.

9 Conséquences

Les conséquences du projet lui-même et celle de la reprise de la directive sont indissociables et sont ainsi présentées ensemble.

9.1 Conséquences financières et en personnel pour la Confédération

A ce stade des travaux, il est difficile d'estimer de manière globale les conséquences financières de l'AP sur le personnel de la Confédération et en particulier sur les ressources du préposé.

Comme cela ressort des réponses du Conseil fédéral à l'interpellation Derder 15.4253 « Protéger les données pour mieux les partager. Une opportunité urgente » et à l'interpellation Aebischer 16.3011 « Adapter non seulement la loi sur la protection des données mais aussi les ressources », le Conseil fédéral entend examiner le besoin en ressources du préposé dans le cadre de son message, une fois que ses nouvelles tâches auront été fixées. Si l'avant-projet est maintenu tel quel, le besoin en ressources du préposé devrait augmenter significativement, en raison des responsabilités découlant notamment des art. 5, 8, 16 et 17, et de son pouvoir décisionnel (art. 41ss AP-LPD). Par ailleurs, compte tenu de la digitalisation croissante de l'économie et de l'administration, il est à prévoir que le nombre de projets privés ou publics et le volume de projets législatifs sur lesquels le préposé doit prendre position augmentent, ce qui entraîne un besoin de ressources supplémentaires. En revanche, dans le cadre de la coopération instaurée par Schengen et par Dublin, le préposé est déjà tenu aujourd'hui de procéder à des contrôles des traitements de données personnelles effectués par les organes fédéraux. Selon ses indications, il effectue actuellement trois à quatre contrôles par année. Ce nombre pourrait légèrement augmenter. Certes le préposé, conformément à la directive (UE) 2016/680, peut désormais rendre des décisions. Les ressources nécessaires à l'exercice de cette nouvelle compétence devraient toutefois rester les mêmes, dans la mesure où le préposé peut aujourd'hui déjà émettre des recommandations à l'intention des organes fédéraux, porter l'affaire pour décision devant l'autorité supérieure si sa recommandation n'est pas suivie et enfin recourir contre la décision de l'autorité supérieure. On ne saurait néanmoins exclure une hausse des demandes de vérification des personnes concernées et des demandes de collaboration des autorités de protection des données des autres Etats Schengen. Quant à l'introduction d'un droit pour les personnes concernées de requérir du préposé l'ouverture d'une enquête, il n'est pas exclu que l'on assiste à une augmentation du nombre de cas. Ces nouvelles tâches pourraient par conséquent nécessiter l'octroi de ressources supplémentaires à concurrence d'un poste voire deux postes au maximum.

Les conséquences financières du projet sur l'administration fédérale devraient être limitées. Il convient toutefois d'examiner cette question en même temps que celle relative aux ressources du préposé.

9.2 Conséquences pour les cantons et les communes

L'acceptation 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 pour 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.

9.3 Conséquences dans le secteur informatique

L'AP 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 toute traitement de données la concernant notamment sur internet ou lorsqu'il prend une décision individuelle automatisée à l'encontre de celle-ci. En outre, s'il envisage d'effectuer des traitements présentant certains risques, il doit procéder à une analyse d'impact 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 documenter ses traitements. Enfin, il doit notifier au préposé et, le cas échéant, également à la personne concernée certains cas de violation de la protection des données.

Les conséquences informatiques pour les organes fédéraux sont plus limitées à différents égards. Ainsi, il est prévu que le devoir d'informer la personne concernée ne s'applique pas lorsque la décision automatisée est prévue par la loi. En outre, les obligations d'établir une étude d'impact du traitement 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 tenu déjà 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). En revanche, la transposition de l'art. 25 de la directive (UE) 2016/680 qui oblige les Etats Schengen à prévoir une obligation d'établir des journaux pour certaines opérations de traitement dans des systèmes automatisés a des conséquences sur les systèmes de traitement automatisés de données tenus par les organes fédéraux. En effet, l'obligation de journalisation prévue à l'art. 10 OLPD doit être adaptée puisque cette norme, dans sa teneur actuelle, s'applique uniquement aux traitements de données sensibles ou de profils de la personnalité lorsque des mesures préventives ne suffisent pas à garantir la protection des données. A cet égard, il y a lieu de prévoir une disposition transitoire, comme l'autorise du reste l'art. 63 par. 2 de la directive (UE) 2016/680. 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. 11a, 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 mais uniquement les activités de traitement des organes fédéraux une fois la nouvelle loi entrée en vigueur.

9.4 Conséquences économiques

L'AP 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. L'AP 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.

L'AP 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 Commis-

sion européenne[153] 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. L'AP 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 108 modernisée 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, l'AP a également pour effet indirect 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, l'AP 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 l'AP pour les responsables du traitement devraient ainsi être compensés, notamment par les avantages découlant du libre transfert des données avec l'Union européenne.

L'intervention de l'Etat est limitée au strict nécessaire, l'idée étant de responsabiliser les responsables du traitement en les encourageant par exemple à respecter des recommandations de bonnes pratiques élaborés par le préposé ou par des organismes 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 garanties ou de règles d'entreprises contraignantes et préalablement approuvées par le préposé.

9.5 Conséquences sociales et sanitaires

Pour répondre aux défis sociétaux que représentent les nouvelles technologies, l'AP prévoit notamment de renforcer les pouvoirs de surveillance du proposé. Il peut ainsi ouvrir une enquête et prendre, le cas échéant des mesures administratives, lorsque par exemple des traitements concernent un grand nombre de personnes et présentent par conséquent un intérêt pour la société en général. Il prévoit également d'attribuer au préposé 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.

9.6 Conséquences sur l'égalité entre hommes et femmes

Aucune conséquence sur l'égalité entre hommes et femme n'est à signaler.

9.7 Conséquences environnementales

Aucune conséquence directe sur l'environnement n'est à signaler.

[153] JO L 215 du 25.8.2000, p. 1.

10 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

10.1 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 - 2019[154].

10.2 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 l'AP fait partie du catalogue des mesures adopté pour la mise en œuvre de la Stratégie Suisse numérique (voir ci-dessus ch. 1.1.3).

11 Aspects juridiques

11.1 Constitutionnalité

11.1.1 Compétence d'approbation de l'échange de notes concernant à 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., art. 24, al. 2 LParl, art. 7a LOGA).

Dans le cas présent, le Conseil fédéral ne dispose d'aucune compétence conférée par la loi ou un traité, car l'art. 35, al. 5 LPD ne s'applique pas. Par ailleurs, il ne s'agit ici pas d'approuver un traité de portée mineure. Il appartient donc à l'Assemblée fédérale de se prononcer sur l'approbation l'échange de notes concernant la reprise de la directive (UE) 2016/680.

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), 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 des art. 141, al. 1, let. d, ch. 3, Cst.

[154] FF **2016** 981, 1097

11.1.2 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.

L'AP 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 peut 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 des art. 141, al. 1, let. d, ch. 3, Cst. pour les mêmes motifs que ceux exposés sous ch. 11.1.1.

11.1.3 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[155], la Constitution fédérale 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.

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 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 fédérale 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 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.

11.2 Compatibilité avec les obligations internationales de la Suisse

L'AP est compatible avec les obligations internationales de la Suisse. Il permet à celle-ci de ratifier le protocole d'amendement de la convention STE 108 dès qu'il sera possible de le faire. 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.

[155] FF **2003** 1915, 1961

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[156].

11.3 Forme de l'acte à adopter

En sus de 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, le présent projet comprend un 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 s'agit d'un acte modificateur unique assujetti au référendum qui réunit sous un titre général d'une part la révision totale de la LPD et d'autre part la révision partielle d'autres actes législatifs de même niveau.

11.4 Frein aux dépenses

L'AP n'implique pas de dépenses qui seraient assujetties au frein aux dépenses (art. 159, al. 3, let. b, Cst.).

11.5 Conformité à la loi sur les subventions

L'AP ne prévoit pas de subventions.

11.6 Délégation de compétences législatives

Le projet prévoit principalement les délégations législatives suivantes :

- En vertu de l'art. 10, al. 2, le Conseil fédéral reste chargé d'édicter des dispositions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité de protection des données.
- Le Conseil fédéral est chargé de régler de manière spécifique 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 (art. 26 AP-LPD).
- Le Conseil fédéral conserve sa faculté d'autoriser, à certaines conditions, le traitement automatisé de données sensibles dans le cadre de projets pilotes (art. 28 AP-LPD).
- Le Conseil fédéral est chargé de régler les droits des personnes concernées en adoptant, dans la réglementation sur l'état civil, des dispositions spéciales qui dérogent tout ou partie à l'art. 34 AP-LPD (art. 45*a*, al. 4, AP-CC).

[156] Considérant 95.