Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police (DFJP)

Office fédéral de la justice (OFJ)
Domaine de direction Droit public
Unité Projets et méthode législatifs

Référence: COO.2180.109.7.150383 / 212.9/2012/00754

Date: 29 octobre 2014

Esquisse d'acte normatif relative à la révision de la loi sur la protection des données

Rapport du groupe d'accompagnement Révision LPD

Table des matières

1. Situation initiale

La loi fédérale du 19 juin 1992 sur la protection des données (LPD ; RS 235.1) est entrée en vigueur le 1er juillet 1993. Elle vise à protéger la personnalité des personnes qui font l'objet d'un traitement de données (art. 1 LPD) et ainsi à garantir le droit fondamental à la sphère privée (art. 13, al. 2, Constitution fédérale, Cst.; RS 101). Elle s'applique au traitement de données personnelles effectué par des personnes privées et par des organes fédéraux (art. 2, al. 1, LPD).

Quelque 20 ans après son entrée en vigueur, la LPD a fait l'objet d'une évaluation détaillée. Il ressort du rapport du Conseil fédéral sur cette évaluation[1] que la loi a permis d'atteindre un niveau de protection appréciable dans les domaines où les défis étaient déjà connus au moment de son entrée en vigueur. Les développements technologiques et sociétaux intervenus depuis lors engendrent cependant depuis quelques années de nouvelles menaces pour la protection des données.

Se fondant sur les conclusions de cette évaluation, 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. Il souhaite plus précisément connaître des mesures permettant d'atteindre les objectifs suivants :

- Assurer la protection des données plus en amont ;
- Sensibiliser davantage les personnes concernées aux risques que représentent les nouvelles technologies pour la protection de la personnalité ;
- Améliorer la transparence des traitements de données ;
- Améliorer le contrôle et la maîtrise des données après leur communication ;
- Protéger les mineurs.

Le Conseil fédéral estime que d'autres possibilités d'intervention sont également dignes d'être examinées, à savoir le renforcement de l'indépendance du Préposé fédéral à la protection des données et à la transparence (PFPDT), l'extension de l'instrument de l'autoréglementation et la répartition des compétences entre Confédération et cantons.

Le DFJP est chargé de soumettre au Conseil fédéral, à la fin de 2014 au plus tard, des propositions sur la suite des travaux. Ce faisant, il doit tenir compte notamment des conclusions de l'évaluation ainsi que des développements en cours dans le domaine de la protection des données dans l'Union européenne et au Conseil de l'Europe. Au sein du DFJP, ce dossier est placé sous la responsabilité de l'Office fédéral de la justice (OFJ).

L'OFJ a institué un groupe de travail élargi afin de disposer des connaissances nécessaires et de tenir compte des intérêts des différents milieux qui pourraient être touchés par la révision de la loi sur la protection des données. Chargé d'accompagner les réflexions sur la réforme, ce groupe comprend des représentants de l'administration fédérale, des cantons, des milieux scientifiques ainsi que des organisations de l'économie et des consommateurs (ci-après : groupe d'accompagnement)[2]. L'OFJ a tenu plusieurs séances avec le groupe

---

[1] Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données (FF 2012 255).

[2] Le groupe d'accompagnement est composé des personnes suivantes: Rolf Reinhard (préposé DFJP Protection des données, LTrans, protection de l'information), Jean-Philippe Walter (PFPDT suppléant), Stephan Brunner

d'accompagnement entre septembre 2012 et octobre 2014. Ils ont étudié la nécessité de modifier la LPD et résumé les résultats de leurs débats dans la présente esquisse d'acte normatif, en se fondant sur les travaux préliminaires d'un groupe de rédaction[3]. L'esquisse d'acte normatif pourrait servir de base à l'avant-projet de révision de la loi sur la protection des données, si le Conseil fédéral décidait de charger le DFJP d'un tel mandat (voir ch. 8). Au vu des nombreux intérêts représentés au sein du groupe d'accompagnement, différentes options sont souvent proposées pour les mesures législatives. Quelques membres du groupe ont en outre déposé une prise de position séparée sur l'esquisse d'acte normatif (cf. annexe).

Par ailleurs, plusieurs interventions parlementaires portant sur la protection des données, et ayant un rapport avec les travaux de révision en cours, sont pendantes devant les Chambres fédérales ou ont été transmises au Conseil fédéral. Elles sont traitées dans l'esquisse d'acte normatif, en rapport avec les thèmes spécifiques sur lesquelles elles portent.

2. Contexte international

Des réformes de la protection des données sont en cours au sein de l'Union européenne (UE) et au sein du Conseil de l'Europe. Le Conseil fédéral estime nécessaire de tenir compte de ces développements dans la réflexion menée au plan national (cf. ch. 1) :

– Modernisation de la Convention STE 108 du Conseil de l'Europe [4]: la Convention STE 108, que la Suisse a ratifiée, fait l'objet d'un profond remaniement. Cette Convention a vocation à devenir un standard universel minimal du fait qu'elle est ouverte à l'adhésion d'États non membres du Conseil de l'Europe et qu'elle constitue actuellement, avec son protocole additionnel[5], le seul texte international contraignant régissant la protection des données. Début 2011, le Conseil de l'Europe a entamé un processus de modernisation de la Convention STE 108. Cette révision poursuit deux objectifs majeurs : gérer les défis de la vie privée qui résultent de l'utilisation des nouvelles technologies de l'information et de la communication et renforcer le mécanisme de suivi et de mise en œuvre de la Convention STE 108. Le projet de modernisation de la Convention STE 108 pourrait être adopté

(Chancellerie fédérale), Thomas Pletscher/Marlis Henze (economiesuisse), Bruno Baeriswyl (préposé à la protection des données du canton de Zurich, président de « Privatim »), Bertil Cottier (Università della Svizzera italiana), Florence Bettschart (Fédération romande des consommateurs), Marc Langheinrich (Università della Svizzera italiana), Dieter Kläy (Union suisse des arts et métiers), David Rosenthal (Verein Unternehmens-Datenschutz), Jacques Vifian (Bureau fédéral de la consommation), Franz Zeller (Office fédéral de la communication), Philippe Künzler (Archives fédérales, à partir de juillet 2014) et Monique Cossali Sauvain (Office fédéral de la justice, présidence du groupe d'accompagnement).

[3] Entre janvier 2014 et juin 2014, une fraction du groupe d'accompagnement (groupe de rédaction) a élaboré un projet pour l'esquisse d'acte normatif. Il était composé des membres suivants: Jean-Philippe Walter (PFPDT suppléant), Stephan Brunner (Chancellerie fédérale), Bertil Cottier (Università della Svizzera italiana), David Rosenthal (Verein Unternehmens-Datenschutz) et Monique Cossali Sauvain (Office fédéral de la justice, présidence du groupe de rédaction). Cet avant-projet a ensuite été examiné et remanié par le groupe d'accompagnement, entre juillet et octobre 2014.

[4] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS 0.235.1).

[5] Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (RS 0.235.11).

et ouvert à la signature dans le courant de 2015.[6] La non-ratification de la Convention modernisée par la Suisse paraît peu réaliste au groupe d'accompagnement. Une telle décision aurait un impact négatif considérable sur les flux transfrontières de données, ce qui aurait des conséquences négatives pour l'économie suisse.

– Paquet de réformes de l'UE : les réformes au plan européen comprennent un projet de *« règlement 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* (ci-après: «projet de règlement UE») »[7] d'une part, et un *projet de « directive relatif 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'exécutions de sanctions pénales, et à la libre circulation de ces données »* (ci-après: «projet de directive UE»)[8] d'autre part. Le projet de règlement UE remplacera la Directive 95/46/CE[9]. Le projet de directive UE remplacera la décision-cadre 2008/977/JAI[10]. Les réformes entreprises par l'UE poursuivent les buts suivants: moderniser le système juridique en matière de protection des données, renforcer les droits des individus, réduire les formalités administratives afin d'assurer une libre circulation des données personnelles dans l'UE et au-delà, améliorer la clarté et la cohérence des règles de l'UE pour la protection des données personnelles et réaliser une application et une mise en œuvre cohérentes et efficaces du droit à la protection des données personnelles dans tous les domaines d'activités de l'UE.

  La Suisse n'est liée par les deux projets susmentionnés que dans la mesure où ils constituent un développement des acquis de Schengen/Dublin. Tel est clairement le cas du *projet de directive UE*. La question est encore ouverte pour ce qui est du *projet de règlement UE*. Dans les domaines qui ne relèvent pas des accords de Schengen/Dublin, la Suisse est considérée comme un État tiers. L'échange de données avec l'UE est alors en principe soumis à la condition que cette dernière reconnaisse à la législation suisse en matière de protection des données un niveau de protection équivalent (décision d'adéquation), ce qui est actuellement le cas. La Suisse, si elle souhaite conserver ce statut, a donc tout intérêt à renforcer sa législation en se rapprochant de la législation européenne, même si elle n'est pas tenue de coller au projet de règlement UE.

  Le calendrier de la réforme de l'UE est encore flou. La phase de trilogue (réunion tripartite informelle à laquelle participent des représentants du Parlement européen, du Conseil et de la Commission) n'a pas encore débuté. La réforme ne devrait pas aboutir avant fin 2015.

---

[6] La dernière séance du comité ad hoc chargé d'examiner le projet de modernisation de la Convention STE 108 (Ad Hoc Committee On Data Protection [CAHDATA]) aura lieu début décembre 2014.

[7] Cf. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52012PC0011&qid=1410779268743> (Proposition de la Commission du 25 janvier 2012).

[8] Cf. <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52012PC0010&qid=1410777949926> (Proposition de la Commission du 25 janvier 2012).

[9] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 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 (JO L 281. p. 31 – 50).

[10] Décision-cadre 2008/977/JAI du Conseil 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 (JO L 350/60, p. 60 – 71).

Les réformes en cours entraînent les conséquences suivantes pour la révision de la LPD:

– Le projet de révision de la LPD faisant suite à l'évaluation de 2011 devrait permettre dans toute la mesure du possible la ratification du projet de modernisation de la *Convention STE 108* (pour autant que la révision de la Convention aboutisse dans un délai raisonnable): la présente esquisse d'acte normatif tient compte des exigences du projet de modernisation dans son état actuel provisoire[11].
– Le *projet de règlement UE*, s'il lie la Suisse, ne le fera que pour les domaines relevant des accords de Schengen/Dublin. La présente esquisse tient malgré tout compte de ses orientations et s'en inspire de manière générale pour tous les traitements de données. La révision de la loi ne saurait en aucun cas aller moins loin que le droit actuel, sous peine de compromettre la décision d'adéquation en vigueur dans les domaines «non Schengen/Dublin».
– Les modifications entraînées par la transposition du *projet de directive UE* se feront vraisemblablement à part, à la fois pour des raisons de calendrier et pour des raisons de clause référendaire (art. 141a al. 2 Cst.), bien qu'une jonction des deux projets ne soit pas exclue. Elles devront se limiter aux modifications liées à la transposition de la directive. Il s'agira d'assurer la cohérence et la coordination des différents travaux de révision ; une esquisse d'acte normatif pour la transposition du projet de directive UE sera soumise à part.

Indépendamment des réformes en cours au niveau européen, la Suisse devra tenir compte des recommandations reçues dans le cadre de la deuxième évaluation Schengen (application correcte des dispositions Schengen relatives à la protection des données) qui a eu lieu en 2014.

Ce contexte de réformes européennes a évidemment des incidences sur le calendrier (cf. ch. 8).

3. Position des membres du groupe d'accompagnement quant à l'existence d'un besoin de légiférer

Il y a fondamentalement deux tendances au sein du groupe d'accompagnement s'agissant du besoin de renforcer la législation en matière de protection des données.

Une *minorité du groupe d'accompagnement*, représentée par les milieux économiques, estime qu'une révision de la LPD ne se justifie pas et que le droit actuel est en l'état suffisant pour garantir les droits et obligations des personnes concernées. Cette partie du groupe d'accompagnement souhaite que le Conseil fédéral attende l'aboutissement des travaux au sein de l'UE et au sein du Conseil de l'Europe et qu'il ne propose que les modifications exigées pour pouvoir accéder au marché (libre circulation des données).

La *majorité du groupe d'accompagnement* estime que la loi actuelle mérite d'être révisée et qu'il convient d'aller de l'avant sans attendre l'entrée en vigueur des révisions au plan européen. Cette fraction préconise par ailleurs une révision plus ambitieuse de la loi, qui ne se limiterait pas aux adaptations exigées pour l'accès au marché. La législation sur la protection des données ne doit en effet pas simplement servir à régir les échanges de données entre particuliers dans une optique commerciale. Elle a une vocation bien plus large, et doit notamment mettre en œuvre le droit constitutionnel de tout un chacun de se déterminer libre-

[11] Version du 18 décembre 2012 (avec les propositions de modernisation adoptées par la 29e réunion plénière» ;cf. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_F_Convention %20108%20modernisée%20version%20F.pdf>).

ment sur les données personnelles qu'il souhaite partager. L'État se doit donc de proposer des mesures efficaces pour concrétiser ce droit, et ce sans attendre qu'on l'y contraigne.

Les membres du groupe d'accompagnement qui sont opposés à la révision de la loi ont néanmoins formulé des remarques s'agissant du présent document, pour le cas où le Conseil fédéral décidait de poursuivre les travaux. Leur avis est ainsi pris en compte dans les opinions exprimées ci-après.

Plusieurs membres du groupe ont souhaité fournir une prise de position ad hoc sur l'esquisse d'acte normatif (cf. annexe).

4. Contenu essentiel de la révision

Les propositions ci-après relatives à l'adaptation de la LPD aux développements technologiques et sociétaux (ou aux menaces que ceux-ci font peser sur la sphère privée) [12] s'insèrent dans l'actuelle structure de la loi. Elles prévoient, outre une partie générale énonçant les principes du traitement des données applicables aussi bien aux organes de la Confédération qu'aux auteurs privés de traitements (voir plus bas, ch. 4.1 à 4.7), des dispositions spécifiques concernant le traitement de données par des particuliers (ch. 4.8) et par les organes fédéraux (ch. 4.9). D'autres propositions concernent l'organisation et les tâches des autorités de contrôle (ch. 4.10), les sanctions pénales (ch. **Erreur ! Source du renvoi introuvable.**) et les dispositions finales (ch. 4.12).

La présente esquisse d'acte normatif ne s'attache en revanche pas en détail au thème du Big Data (« mégadonnées ou données massives »). On parle de Big Data lorsqu'une grande quantité de données provenant de différentes sources sont saisies et enregistrées à l'aide de systèmes de traitement à très haut débit, en vue de permettre leur exploitation et leur analyse sans but prédéterminé et sans limite de temps[13]. Le Big Data implique de nouveaux enjeux pour le droit sur la protection des données (p. ex. eu égard aux principes de reconnaissabilité et de finalité ou à la ré-individualisation de données anonymes). Les conséquences du Big Data ne sont toutefois pas encore bien connues. Jusqu'ici, la doctrine juridique n'a traité en détail que quelques aspects de cette problématique[14]. En conséquence, la présente esquisse d'acte normatif ne propose pas de solutions globales, mais uniquement des mesures ponctuelles permettant de s'attaquer aux défis que le Big Data pose en matière de protection des données[15]. Un examen approfondi des implications du Big Data pour la protection des données pourrait avoir lieu dans le cadre des travaux de mise en œuvre de la

---

[12] Les mesures de protection des données peuvent entrer en conflit avec d'autres intérêts. Lors de l'examen de mesures législatives en la matière, il convient par conséquent de tenir compte non seulement de la protection de la personnalité, mais encore d'autres intérêts concernés (en particulier intérêts de l'économie, droit à la liberté d'opinion et d'information ainsi que d'autres intérêts spécifiques, tant privés que publics). Voir à ce propos le rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 267 et 269.

[13] Cf. la définition de ce terme sur le site du PFPDT http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=fr .

[14] Cf. BAERISWYL, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber/Thouvenin (édit.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zurich etc., 2014, pp. 46 ss.

[15] En font notamment partie les propositions de réglementation relatives au principe du « Privacy by Design » (cf. ch. 4.3.2), à l'analyse de l'impact potentiel du traitement de données (cf. ch. 4.3.2), au droit d'accès relatif à la structure logique du traitement des données (cf. ch. 4.4.3) ou aux décisions individuelles automatisées (cf. ch. 4.4.6).

motion Rechsteiner 13.3841 « Commission d'experts pour l'avenir du traitement et de la sécurité des données »[16].

4.1 Concept et mise en œuvre

4.1.1 Concept

Le groupe d'accompagnement propose de conserver une seule loi pour les secteurs privé et public. La garantie d'un développement coordonné et harmonieux de la protection des données en droit privé et en droit public passe en effet par une réglementation commune des problèmes inhérents aux deux domaines. Dans cette perspective, le groupe d'accompnement a, dans la mesure du possible, harmonisé les règles pour les deux secteurs afin de créer un cadre commun pour le traitement des données personnelles, et prévu des solutions différentes uniquement lorsque cela était indispensable.

Le but de la loi restera inchangé. La future loi devra conserver son caractère technologiquement neutre et se limiter comme maintenant à fixer des principes généraux, ceci afin de s'appliquer à une palette de situations la plus large possible.

L'idée de regrouper dans la loi tout ou partie des dispositions contenues dans les lois spéciales (sorte de codification du droit de la protection des données au niveau fédéral) a été abandonnée : de l'avis du groupe d'accompagnement, cela n'apporterait aucune plus-value. Un examen de la législation fédérale a révélé que la grande majorité des dispositions de protection des données contenues dans les lois spéciales visent à créer une base légale spécifique pour le domaine concerné ou à concrétiser les principes de la LPD pour le domaine concerné. Elles ne peuvent dès lors pas être remplacées par des dispositions générales dans la LPD, et les rassembler dans un code n'apporterait aucun avantage du point de vue légistique.

4.1.2 Mise en œuvre

a) Renforcement des pouvoirs de l'autorité de contrôle et facilitation de l'accès à la justice pour les particuliers

Une majorité du groupe d'accompagnement estime que le rapport d'évaluation du Conseil fédéral a montré des lacunes dans la mise en œuvre (« Durchsetzung ») de la LPD. Ces dernières sont principalement dues au fait que notre autorité de contrôle[17], en l'occurrence le PFPDT n'a aujourd'hui que peu de pouvoirs, et au fait que les personnes concernées font rarement valoir leurs droits en justice, vu la disproportion entre le bénéfice d'une éventuelle victoire judiciaire et les risques – principalement financiers – et les efforts liés à l'ouverture d'une procédure. Ces deux facteurs nuisent à une application effective de la loi, et condui-

[16] La motion Rechsteiner 13.3841 « Commission d'experts pour l'avenir du traitement et de la sécurité des données », que le Parlement a transmise le 4 juin 2014, charge le Conseil fédéral d'instituer une commission d'experts interdisciplinaire pour répondre à des questions relatives aux développements technologiques et politiques dans le domaine du traitement et de la sécurité des données, et d'en étudier l'importance pour l'économie, la société et l'État suisses. Ce groupe d'experts doit également formuler des recommandations pour la Suisse. La responsabilité de ce dossier incombe au Département fédéral des finances (DFF).

[17] Des propositions sont formulées au ch. 4.10 de la présente esquisse d'acte normatif pour adapter les tâches et les compétences / l'organisation de l'autorité de contrôle. La terminologie choisie pour la future surveillance de la protection des données s'aligne sur celle des réformes de l'UE et du Conseil de l'Europe, ce qui évite aussi de déterminer la forme de l'organisation par un choix linguistique. On parlera d' « autorité de contrôle ».

sent à une perte de contrôle et de maîtrise des données. Elles impliquent qu'une grande partie des cas de violation de la LPD ne sont pas constatés et perdurent. De plus, l'effet préventif de la loi est fortement diminué dans la mesure où les responsables de traitements, qui n'ont que peu de raison de craindre d'être remis à l'ordre, peuvent être tentés de ne pas tenir compte de cette éventualité dans leur comportement. Une meilleure mise en œuvre de la loi passe donc par un renforcement des pouvoirs de l'autorité de contrôle, soit l'octroi d'une compétence de rendre des décisions, voire de prononcer des sanctions et/ou par un renforcement des droits, principalement procéduraux, des personnes concernées.

La majorité du groupe est favorable à un renforcement des pouvoirs de l'autorité de contrôle. Elle estime en effet que le déséquilibre croissant et systématique dans les rapports entre les personnes concernées et les auteurs de traitements – souvent de grandes entreprises – qui se concrétise notamment par des politiques de traitement de données peu transparentes, voire par l'absence de possibilité de librement choisir l'utilisation qui sera faite de ces données, commande plus que de simples recommandations. Ce constat a déjà été fait dans de nombreux pays européens, tels la France, l'Italie, la Grande-Bretagne, la Suède ou l'Espagne, où les autorités de contrôle ont la faculté de rendre des décisions contraignantes, voire de prononcer des amendes.[18] Dans un monde globalisé où les échanges internationaux de données sont de plus en plus fréquents, il est primordial que notre autorité de contrôle dispose de moyens comparables à ceux de ses homologues étrangers. Notons aussi que le projet de modernisation de la Convention STE 108 prévoit que les autorités de contrôle disposent de pouvoirs de décision (un tel pouvoir est par ailleurs aussi prévu par le projet de directive UE [art. 46)] et le projet de règlement UE [art. 53]). Si le texte est adopté, et que la Suisse souhaite le ratifier, elle devra donc prévoir une telle compétence dans sa législation. Enfin, dans le cadre de la deuxième évaluation Schengen, l'UE a recommandé à la Suisse de doter le PFPDT du pouvoir de rendre des décisions contraignantes. Dans ses observations, l'UE a encore ajouté que le renforcement des pouvoirs de sanction du PFPDT serait le bienvenu.

Le groupe d'accompagnement est en revanche plus mitigé s'agissant de la question du renforcement des droits des personnes concernées. *Une partie* estime que les possibilités de faciliter l'accès à la justice pour les personnes concernées sont trop compliquées à mettre en œuvre et trop peu efficaces (voir les réflexions menées dans le cadre des prétentions des parties aux ch. 4.8.3 et 4.9.5) pour mériter que l'on entreprenne de gros chantiers. Par ailleurs, il ressort de l'évaluation de la LPD que les droits actuellement inscrits dans la loi sont, en comparaison internationale, déjà plutôt bien développés[19]. Cette fraction du groupe préconise donc de privilégier un renforcement significatif des pouvoirs de l'autorité de contrôle, et d'améliorer ponctuellement les droits des personnes concernées. *Une autre partie du groupe d'accompagnement* estime quant à elle qu'il existe des mesures efficaces pour renforcer l'accès des personnes concernées à la justice et qu'il convient aussi de les proposer. La protection des droits des individus est en effet un problème avéré selon le rapport d'évaluation. Pour cette partie du groupe, il s'agit également de parer à l'éventualité que les propositions relatives au renforcement du rôle de l'autorité de contrôle soient refusées au

[18] Cf. Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 172 et 213 s.; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

[19] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 72 ss., 212 s.; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

cours du processus législatif en raison des ressources supplémentaires qu'elles nécessiteraient.

Une minorité du groupe d'accompagnement estime quant à elle qu'il n'est pas nécessaire de renforcer les pouvoirs de l'autorité de contrôle ni les moyens à disposition des personnes concernées pour faire valoir leurs droits. Des éventuelles modifications législatives ne doivent intervenir à ses yeux que dans la mesure de ce qui est nécessaire, en regard du droit UE et du projet de modernisation de la Convention STE 108, pour l'accès au marché (cf. ch. 3).

b) Règles plus détaillées

Le caractère général et technologiquement neutre des règles de la LPD entraîne, dans le secteur privé surtout, une certaine incertitude quant aux comportements à adopter, tant pour les auteurs de traitements que pour les personnes concernées, ce qui nuit à la mise en œuvre efficace de la loi. Afin de remédier à cette problématique et d'améliorer la prévisibilité du droit, le groupe d'accompagnement propose de compléter les principes généraux de la loi par des dispositions plus détaillées, applicables au secteur privé, voire au secteur public. On pourrait ainsi avoir des règles détaillées sur des thèmes qui suscitent aujourd'hui de nombreuses questions, comme la vidéosurveillance, le « Big Data », le commerce électronique ou le « Cloud Computing ». Ces règles permettraient également de préciser des notions figurant dans la loi (p. ex : « risque accru », cf. ch. 4.3.2) ou les modalités de certains droits (par ex: le droit à l'effacement, cf. ch. 4.4.5).

La question est de savoir si ces dispositions doivent êtres contraignantes ou non. Les deux tendances sont représentées dans le groupe d'accompagnement :

- Les règles contraignantes auraient l'avantage d'obliger directement leurs destinataires. Leur élaboration susciterait toutefois de nombreuses questions en lien avec le principe de la légalité (délégation de compétences, densité normative, légitimité de l'autorité qui les édicterait), et leur modification prendrait du temps, dans la mesure où il faudrait passer par le processus normal de modification des ordonnances interne à l'administration fédérale.
- Les règles non contraignantes (« bonnes pratiques », « bons usages ») seraient moins problématiques sous l'angle principe de la légalité. Elles sont modifiables très rapidement, et laissent une marge de manœuvre pour les responsables de traitements qui peuvent aussi appliquer d'autres règles. Pour inviter les auteurs de traitements à suivre ces règles, on pourrait instituer une présomption légale selon laquelle un traitement est licite pour autant que son auteur ait respecté les règles de bonnes pratiques. Cette présomption vaudrait pour les auteurs de traitements privés et publics. On pourrait par exemple s'inspirer de l'art. 52a de l'ordonnance sur la prévention des accidents professionnels (OPA; RS 832.30). Cette disposition prévoit que l'employeur est présumé se conformer aux prescriptions sur la sécurité au travail s'il observe les directives émises par la commission de coordination (al. 2). L'employeur peut cependant aussi se conformer aux prescriptions sur la sécurité au travail d'une autre manière que celle qui est prévue par les directives, s'il prouve que la sécurité des travailleurs est également garantie (al. 3). Non contraignantes, ces règles de bonnes pratiques reposeraient toutefois principalement sur la bonne volonté de leurs destinataires, ce qui pourrait réduire leur efficacité.

Une majorité du groupe d'accompagnement propose que l'élaboration de ces règles (contraignantes ou non contraignantes) soit confiée à un comité spécialisé (ci-après: « comité »),

distinct de l'autorité de contrôle au sens étroit (cf. aussi ch. 4.10.2, let. c, et ch. 4.10.3). Cet organe serait composé d'experts indépendants, et non de représentants des milieux concernés.[20] Les milieux intéressés seraient consultés pour l'élaboration des règles. Le comité pourrait aussi leur donner mandat d'élaborer eux-mêmes de telles règles. Les milieux concernés pourraient par ailleurs soumettre spontanément leurs règles pour approbation au comité.[21] Dans tous les cas, ces dernières seraient mises en consultation auprès des associations de protection des consommateurs.

- Variante: Le comité ne pourrait élaborer des règles de bonnes pratiques que si le mandat donné aux milieux concernés de le faire eux-mêmes n'est pas réalisé dans un certain délai.

Une *minorité du groupe* s'oppose à l'institution d'un comité spécialisé, qui engendrerait des charges administratives et financières supplémentaires et affaiblirait la protection des données. Elle propose que cette compétence soit conférée à l'autorité de contrôle elle-même (cf. ch. 4.10.3).

4.2 Champ d'application et terminologie

4.2.1 Champ d'application

a) Champ d'application personnel

La loi sur la protection des données régit le traitement de données personnelles, aussi bien par des personnes privées que par des organes fédéraux (cf. art. 2, al. 1, LPD). La LPD ne s'applique toutefois pas au traitement de données personnelles par des organes cantonaux, sous réserve de l'art. 37 LPD. La question de l'adéquation de cette répartition des compétences[22] entre Confédération et cantons a également été examinée ici. Le groupe d'accompagnement s'est demandé, dans une perspective d'harmonisation, s'il ne faudrait pas étendre le champ d'application de la LPD aux organes cantonaux. Une telle extension de la compétence législative de la Confédération en matière de protection des données requérrait une révision de la Constitution fédérale.

Une consultation effectuée par la Conférence des gouvernements cantonaux (CdC) auprès des cantons à la demande de la cheffe du DFJP a montré que la majorité des cantons ne sont pas favorables à l'extension du champ d'application de la loi aux traitements de données effectués par les organes cantonaux. Lors du Dialogue confédéral de l'automne 2013, la cheffe du DFJP a déjà fait savoir aux cantons qu'elle ne poursuivrait pas l'idée d'une unifi-

---

[20] La loi – respectivement l'ordonnance – devra encore prévoir notamment des règles sur l'élection, la période de fonction ou les conflits d'intérêts des membres du comité, ainsi que sur la position de ce dernier par rapport à l'autorité de contrôle elle-même.

[21] La loi fédérale autrichienne sur la protection des données se rapportant à des personnes (Datenschutzgesetz 2000) connaît une procédure allant dans ce sens. Le § 6, al. 4, stipule ainsi: « Pour définir plus précisément ce qui doit être considéré comme une utilisation de données de bonne foi dans les différents domaines, il est possible, pour le secteur privé, de confier à des organismes professionnels de représentation légale, à d'autres associations professionnelles ou à des institutions similaires le soin d'élaborer des règles de comportement. De telles règles ne peuvent être publiées qu'après avoir été soumises au chancelier fédéral, qui doit en examiner la conformité avec les dispositions de la présente loi fédérale et constater que tel est le cas. » (traduction non officielle).

[22] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 268.

cation du droit de la protection des données. Le champ d'application devrait donc à l'avenir se limiter, comme aujourd'hui, aux traitements de données effectués par des organes fédéraux et par des privés, de même que par des organes cantonaux en exécution du droit fédéral aux conditions de l'art. 37 LPD.

La LPD s'appliquera comme aujourd'hui aux médias. Une attention particulière sera cependant portée au besoin de prévoir des dispositions spéciales afin de protéger le secret de rédaction, en particulier dans le cadre du droit d'accès (cf. ch. 4.4.3). Il faudra aussi tenir compte de l'intérêt des médias dans le cadre du « droit à l'oubli » (cf. ch. 4.4.5).

b) Champ d'application à raison de la matière

La loi sur la protection des données d'applique au traitement de données concernant des personnes physiques et morales (art. 2, al. 1, LPD). Elle se distingue ainsi de la Convention STE 108 et de la législation de plusieurs États européens, qui ne protègent que les personnes physiques. Le groupe d'accompagnement a donc examiné s'il était justifié de maintenir cette protection pour les personnes morales.

Une majorité du groupe d'accompagnement a conclu que la LPD devait continuer de s'appliquer aux données de personnes morales. Elle estime que l'exclusion de ces dernières ne cadrerait pas avec le système juridique suisse, en vertu duquel les personnes morales bénéficient de la protection de la personnalité garantie par le code civil (art. 53 en relation avec les art. 28 ss CC [RS 210]). La majorité du groupe d'accompagnement considère au surplus que la non-application de la LPD aux données de personnes morales pourrait aboutir à des résultats problématiques. Elle souligne que les entreprises familiales et les petites entreprises surtout peuvent avoir besoin que leurs données soient protégées au même titre que les données de personnes physiques, notamment lorsque les informations relatives à la personne morale ont un rapport avec les personnes physiques la dirigeant.

La proposition de la majorité du groupe d'accompagnement prévoit toutefois que le traitement de données de personnes morales dans le cadre de leurs activités commerciales soit ajouté à la liste des intérêts privés prépondérants de l'art. 13, al. 2, LPD (cf. plus bas, ch. 4.8.2). Cette solution faciliterait les transactions commerciales dans la pratique, sans compromettre par trop la protection des données des personnes morales. Il ne s'agirait pas d'un motif justificatif absolu (pas plus que les autres intérêts énumérés à l'art. 13, al. 2, LPD) qui autoriserait en soi un traitement de données. Il faudrait ici également procéder à une pesée des intérêts, en tenant compte de toutes les circonstances du cas particulier. Lorsque le traitement porte sur des données ne concernant pas les activités commerciales, les personnes morales disposeraient d'ailleurs de tous les moyens de droit prévu par la LPD.

Enfin, pour faciliter les échanges de données transfrontières avec des pays dont l'ordre juridique ne protège pas les données personnelles de personnes morales, la majorité du groupe d'accompagnement propose d'arrêter dans la loi que l'adéquation de la protection des données selon l'art. 6 LPD n'implique pas que la législation étrangère protège les données personnelles de personnes morales (cf. plus bas, ch. 4.5).

Une minorité du groupe d'accompagnement souhaite que les données personnelles de personnes morales soient entièrement exclues du champ d'application de la LPD. Elle motive son choix par le fait que la législation de nombreux États européens, de même que le projet de modernisation de la Convention STE 108 protègent exclusivement les droits des personnes physiques. Elle estime en outre que la protection de la personnalité des personnes morales est déjà assurée à satisfaction par le CC (art. 28 ss), la loi fédérale contre la concurrence déloyale (LCD ; RS 241) et le secret d'affaires. Il serait dans tous les cas envisageable de soumettre les données personnelles des personnes morales à la LPD lorsqu'une personne physique est reconnaissable comme propriétaire d'une entreprise individuelle.

c) Champ d'application territorial

L'évaluation de la LPD a révélé que la dimension internationale du traitement des données ne cessait de gagner en importance en raison des développements technologiques. Les traitements transfrontières de données sont de plus en plus fréquents, ce qui débouche sur des situations complexes et peu transparentes pour les personnes concernées et pour les autorités de contrôle, ainsi que pour les auteurs de traitements[23]. Le groupe d'accompagnement s'est par conséquent demandé si ces nouveaux défis appellaient une adaptation du champ d'application territorial de la LPD (en particulier en ce qui concerne l'applicabilité de la loi à des faits de portée internationale).

L'actuelle LPD ne contient aucune disposition définissant explicitement son champ d'application territorial. Le droit international privé fournit des règles de conflits de loi spéciales pour les dispositions de droit privé de la LPD. La loi fédérale sur sur le droit international privé (LDIP; RS 291) définit notamment les compétences des tribunaux ou des autorités suisses en matière de protection des données, sous réserve de traités internationaux (art. 129, al. 1[24] et 130, al. 3, LDIP[25]) ainsi que les prétentions fondées sur une atteinte à la personnalité liées au traitement de données personnelles (cf. en particulier art. 139 LDIP[26]). Selon le groupe d'accompagnement, cette réglementation permet d'appliquer les dispositions de droit privé de la LPD de manière assez large (soit aussi à certains traitements de données à l'étranger). Il ne propose par conséquent aucune modification dans ce domaine.

Le droit public par contre ne connaît pas de règles spécifiques de conflits de lois internationaux. C'est le principe de la territorialité qui s'applique aux dispositions de droit public de la LPD, à savoir que le droit suisse ne s'applique qu'aux faits qui se produisent en Suisse. Selon la jurisprudence du Tribunal fédéral, le droit public suisse peut, dans certaines circonstances, être appliqué aussi à des faits survenus à l'étranger lorsque ceux-ci ont des répercussions suffisantes sur le territoire suisse (principe des effets)[27]. *Une majorité du groupe d'accompagnement* propose de codifier explicitement cette jurisprudence dans la LPD pour

---

[23] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données, FF 2012 255, 260 s., 267.

[24] Art. 129, al. 1, LDIP: « Les tribunaux suisses du domicile ou, à défaut de domicile, ceux de la résidence habituelle du défendeur sont compétents pour connaître des actions fondées sur un acte illicite. Sont en outre compétents les tribunaux suisses du lieu de l'acte ou du résultat et, pour connaître des actions relatives à l'activité de l'établissement en Suisse, les tribunaux du lieu de l'établissement. »

[25] Art. 130, al. 3, LDIP: « Les actions en exécution du droit d'accès dirigées contre le maître du fichier peuvent être intentées devant les tribunaux mentionnés à l'art. 129 ou devant les tribunaux suisses du lieu où le fichier est géré ou utilisé. »

[26] En vertu de l'art. 139, al. 3, en relation avec l'al. 1 LDIP, les prétentions fondées sur une atteinte à la personnalité résultant du traitement de données personnelles sont régies, « au choix du lésé: a. par le droit de l'État dans lequel le lésé a sa résidence habituelle, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État ; b. par le droit de l'État dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle, ou c. par le droit de l'État dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet État. »

[27] Pour le principe des effets comme particularité du principe de territorialité, voir en particulier ATF 133 II 331, 341 consid. 6.1. S'agissant du droit sur la protection des données, le Tribunal fédéral a retenu, par exemple dans ATF 138 II 346, 352 s. consid. 3.3 (« Google Street View »), que les images qui ont été prises en Suisse et sont 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.

le droit public de la protection des données[28]. L'intention est de souligner que la LPD s'applique également à des faits qui ont des répercussions en Suisse, même si le traitement des données a lieu à l'étranger. De tels faits doivent en outre relever du domaine de compétence de l'autorité de contrôle. *Une minorité du groupe d'accompagnement* se prononce contre cette proposition. Elle est d'avis qu'une codification de la jurisprudence du Tribunal fédéral relative aux principes de territorialité et des effets déboucherait sur une insécurité juridique. Elle relève qu'il n'y a pas non plus de définition légale du principe de territorialité dans d'autres domaines du droit. Cette solution entraînerait des incertitudes sur la question de savoir si et dans quelle mesure la jurisprudence du Tribunal fédéral continuera à s'appliquer à la protection des données. On risquerait d'aboutir à des divergences – non prévues par le groupe d'accompagnement – par rapport à la pratique du Tribunal fédéral.

Etant donné que la LPD peut être appliquée aussi à des auteurs de traitements de données qui n'ont pas de domicile (siège) en Suisse, le groupe d'accompagnement propose en outre d'obliger, dans certains cas, ces personnes à indiquer une adresse de correspondance en Suisse afin d'accélérer la procédure (cf. plus bas, ch. 4.10.2 let. a/aa).

d) Exceptions au champ d'application

da) Traitement à des fins exclusivement personnelles

L'exception prévue à l'actuel art. 2, al. 2, let. a, LPD devrait être adaptée à l'art. 3, al. 1bis, du projet de modernisation de la Convention STE 108[29]. Le groupe d'accompagnement propose de supprimer la condition de la non-communication à des tiers, et de reformuler la disposition en ce sens que la LPD ne s'applique pas aux traitements de données effectués par une personne physique pour des activités exclusivement personnelles. Sont ici visées principalement les communications à des parents et des amis proches. Les « amis » sur les réseaux sociaux[30] n'entrent pas dans cette catégorie s'il n'y a pas de lien étroit.

db) Autres exceptions

Vu le statut particulier dont jouit le Comité international de la Croix-Rouge (CICR), le groupe d'accompagnement propose de maintenir l'actuelle clause d'exception de l'art. 2, al. 2, let. e, LPD, qui exclut du champ d'application de la loi les données personnelles traitées par celui-là. Le groupe d'accompagnement part donc du principe qu'une telle dérogation restera possible selon le projet de modernisation de la Convention STE 108. La raison de cette exception réside dans le fait que le CICR est de plus en plus reconnu comme un sujet de droit international public et que ces sujets ne peuvent pas être soumis sans autre au droit interne d'un Etat[31]. La doctrine critique notamment le fait que d'autres organisations internationales ne soient pas mentionnées dans cette clause d'exception de la LPD, soulignant que cette différence de traitement est problématique en regard du principe d'égalité inscrit dans la

---

[28] On trouve une disposition analogue dans le droit sur la concurrence par exemple, à l'art. 2, al. 2, de la loi sur les cartels (LCart; RS 251): « La présente loi est applicable aux états de fait qui déploient leurs effets en Suisse, même s'ils se sont produits à l'étranger. »

[29] Art. 3, al. 1bis, du projet de modernisation de la Convention STE 108: « La présente Convention ne s'applique pas aux traitements de données effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

[30] Sur la problématique des réseaux sociaux, voir le rapport du Conseil fédéral « Cadre légal pour les médias sociaux: Rapport en réponse au postulat Amherd 11.3912 du 29 septembre 2011 ».

[31] Cf. le message du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421, 447 s..

Constitution (art. 8 Cst.)[32]. Dans le message du 19 février 2003 relatif à la révision de la LPD[33], le Conseil fédéral avait exprimé l'intention d'exclure expressément du champ d'application de la LPD toutes les organisations internationales établies sur le territoire de la Confédération avec lesquelles un accord de siège a été conclu. Cette réglementation n'a toutefois pas été reprise par la Parlement, raison pour laquelle le groupe d'accompagnement ne propose pas non plus, dans le cadre des présents travaux, une extension dans ce sens de l'art. 2, al. 2, let. e, LPD.

Les autres exceptions au champ d'application de la LPD ne pourront à notre sens être maintenues que si les exigences du projet de modernisation de la Convention STE 108 sont remplies dans le domaine concerné. Ce projet abroge la possibilité pour les États de faire des réserves concernant le champ d'application de la Convention [34].

- Le groupe d'accompagnement est d'avis que l'exception concernant les registres publics relatifs aux rapports juridiques de droit privé doit être supprimée (art. 2, al. 2, let. d, LPD), et ce pour plusieurs raisons. D'abord, le fait que ces domaines soient régis par des lois spéciales ne justifie pas une exception. En effet, d'autres secteurs, bien que réglés par des lois spéciales, sont aussi soumis à la LPD (p. ex : le casier judiciaire). Ensuite, cette exclusion est aujourd'hui artificielle dans la mesure où le PFPDT est très souvent sollicité dans ces domaines pour des questions relevant justement de la LPD. Enfin, ces matières sont bien souvent imbriquées avec d'autres, qui, elles, sont soumises à la LPD, ce qui rend la dichotomie difficile à mettre en œuvre. Il sera toujours possible de tenir compte des particularités des registres dans des dispositions spéciales.
- Pour les autres exceptions (soit l'art. 2, al. 2, let. b et c, LPD), il faudrait examiner si elles restent valables, si elles doivent être modifiées ou si les exigences du projet de modernisation de la Convention STE 108 (voire du droit UE) doivent être transposées dans les législations spéciales. Deux options concrètes sont ressorties des discussions au sein du groupe d'accompagnement : soit on supprime les exceptions et le domaine est alors soumis à la LPD, soit on les maintient et on vérifie que les lois spéciales sont à niveau.

4.2.2 Définitions

Le groupe d'accompagnement propose de maintenir la définition actuelle de « données personnelles » (art. 3, let. a, LPD) ainsi que celle de « fichier » (art. 3, let. g, LPD) et de « communication » (art. 3, let. f, LPD). Il ne voit en effet aucune raison de modifier ces notions, qui sont aujourd'hui bien intégrées dans la pratique des autorités de contrôle et des tribunaux suisses.

La liste des définitions et la terminologie devront au besoin être adaptées à celle du projet de modernisation de la Convention STE 108. Cela vaut en particulier pour la définition des « données sensibles » (art. 3, let. c, LPD). Le projet prévoit d'y inclure les données génétiques et les données biométriques. Pour éviter d'aller trop loin (p. ex. pour que toute photo ne soit *per se* considérée comme une donnée sensible), on pourrait restreindre la définition sur le modèle de l'art. 6, al. 1, du projet de modernisation de la Convention STE 108[35]. Le

---

[32] Cf. MAURER-LAMBROU/KUNZ, in: « Basler Kommentar DSG/BGÖ », 3e éd., Bâle 2014, N 41 ad art. 2 LPD.

[33] Cf. FF 2003 1915, 1926 s.

[34] La Suisse, au moment de son adhésion à l'actuelle Convention STE 108, avait déclaré que celle-ci ne s'appliquait pas aux fichiers constitués et utilisés par les parlements fédéral et cantonaux dans le cadre de leurs délibérations et aux fichiers du Comité international de la Croix-Rouge ; RO 2002 2847, 2869.

[35] Art. 6, al. 1, du projet de modernisation de la Convention STE 108 : « Le traitement de données génétiques ou

groupe d'accompagnement propose au surplus de prévoir, si les personnes morales devaient être maintenues dans le champ d'application de la loi (ch. 4.2.1, let. b), que seules les données concernant les personnes privées sont susceptibles d'être considérées comme sensibles.

S'agissant du terme « maître du fichier »/« Inhaber der Datensammlung » (art. 3, let. i, LPD), le groupe d'accompagnement a débattu de l'opportunité d'aligner la terminologie sur celle de la Convention STE 108 et du droit européen, qui utilisent la notion respectivement de « responsable du traitement »[36] et « für die Verarbeitung Verantwortlichen »[37]. Les conséquences matérielles d'une telle adaptation, étant donné que les notions utilisées dans le droit suisse et dans le droit européen ne se recoupent pas totalement, doivent encore être examinées en détail. Un alignement terminologique ne doit pas déboucher sur une insécurité juridique.

Il pourrait être opportun de définir dans la loi les notions de « sous-traitants » et de « destinataires ». Dans le cas contraire, la formulation de l'actuel art.10a LPD pourrait être revue afin d'éviter une confusion avec la notion de « tiers » utilisée dans d'autres dispositions (p. ex: art. 9, 12, 13 ou 14 LPD).

Le groupe d'accompagnement propose enfin d'abandonner la notion de « profils de la personnalité », qui est propre à la Suisse et qui a peu d'effets en pratique, dans la mesure où les obligations particulières liées à l'existence de tels profils (p. ex : art. 4, al. 5, et 14 LPD) sont rarement respectées, principalement dans le secteur privé. Le groupe d'accompagnement propose d'appréhender la problématique par des moyens plus efficaces, tels une règlementation sur les décisions automatisées (ch. 4.4.6) ou une approche fondée sur le risque (cf. ch. 4.3.2).

4.3 Principes généraux de protection des données personnelles

4.3.1 Transparence des traitements

Actuellement, la question de la reconnaissabilité de la collecte des données et celle du devoir d'information sont réglées à des endroits différents, soit à l'art. 4, al. 4, LPD, et aux art. 14 (secteur privé) et 18 à 18b LPD (organes fédéraux). *Une majorité du groupe d'accompagnement* propose de traiter ces deux thèmes dans une seule et même disposition, applicable aux secteurs privé et public, ce qui aurait le mérite de simplifier la loi et d'éviter les redondances. Cette disposition prévoirait une *obligation d'informer* pour toutes les catégories de données traitées, comme c'est déjà le cas actuellement pour le secteur public (et comme cela est prévu par le projet de modernisation de la Convention STE 108[38] et le droit de l'UE[39]). On renoncerait donc à faire une distinction entre données sensibles et données non sensibles. La personne concernée devrait être informée – dans la mesure où elle ne l'est pas déjà – des données qui sont collectées et dans quel but elles le sont, des éventuelles caté-

---

de données concernant des infractions, condamnations pénales et mesures de sûreté connexes, le traitement de données biométriques identifiant un individu de façon unique, ainsi que le traitement de données à caractère personnel pour les informations qu'elles révèlent sur l'origine raciale, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres convictions, la santé ou la vie sexuelle, n'est autorisé qu'à la condition que la loi applicable prévoit des garanties appropriées, venant compléter celles de la présente Convention. »

[36] Cf. art. 2, let. d, du projet de modernisation de la Convention STE 108.

[37] Cf. art. 4, al. 5, du projet de règlement UE ainsi que l'art. 3, al. 6, du projet de directive UE.

[38] Cf. art. 7bis du projet de modernisation de la Convention STE 108.

[39] Cf. art. 14 du projet de règlement UE et art. 11 du projet de directive UE.

gories de destinataires ainsi que des droits qui lui sont conférés par la loi. Les coordonnées du responsable du traitement devraient par ailleurs lui être communiquées afin qu'elle puisse le contacter. Le devoir d'information serait réputé être respecté s'il découle manifestement des circonstances que la personne devrait avoir connaissance de tous les éléments pertinents. Les modalités de ce devoir pourraient être précisées dans des règles de bonnes pratiques ou dans des règles contraignantes (cf. ch. 4.1.2, let. b). Outre le cas où la personne concernée a déjà été informée, il conviendrait de prévoir une exception au devoir d'informer lorsque le traitement est prévu par la loi ou lorsque l'information implique des efforts disproportionnés, ou encore lorsqu'il s'agit de préserver la vie ou l'intégrité corporelle de la personne concernée ou d'un tiers. La disposition concernant le devoir d'information serait conçue comme un principe de traitement des données.

Une minorité du groupe d'accompagnement s'oppose à l'introduction d'un devoir général d'information. Elle estime, notamment, que cela représenterait une charge de travail disproportionnées pour les entreprises.

Un autre instrument important de la transparence des traitements est le droit d'accès de la personne concernée, qu'elle peut exercer auprès du maître du fichier. Le groupe d'accompagnement propose de renforcer ce droit. Ce thème est abordé plus loin, au ch. 4.4.3.

4.3.2 Mesures de diligence

Conformément à ce que prévoient les art. 7 et 8bis, al. 2, 3 et 4, du projet de modernisation de la Convention STE 108, et de manière à mettre en œuvre les postulats Schwaab 13.3806 « La protection de la sphère privée doit être garantie par défaut » et 13.3807 « Un renforcement de la protection des données grâce au „privacy by design" »[40] et le postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication »[41], le groupe d'accompagnement propose d'introduire une obligation pour le responsable du traitement ou, le cas échéant, pour le sous-traitant, de prendre certaines mesures afin de prévenir les violations de la loi[42] et de les éliminer, ou d'en réduire les conséquences[43].

Les devoirs de diligence suivants en font notamment partie :

– Mesures d'ordre technique et organisationnel garantissant la sécurité des données.

---

[40] Les postulats Schwaab 13.3806 et 13.3807 du 25 septembre 2013 n'ont pas encore été traités par le Conseil national.

[41] Le postulat Recordon 13.3989 du 27 septembre 2013 a été adopté par le Conseil des Etats le 11 décembre 2013.

[42] À ce propos, il conviendra d'étudier, lors de la suite des travaux de révision de la LPD, si le principe de précaution, qui prend ses racines dans le droit environnemental, ne pourrait pas être repris comme principe général dans le domaine de la protection des données. Concernant le principe de précaution dans le droit de l'environnement, voir en particulier l'art. 1, al. 2, de la loi sur la protection de l'environnement (LPE; RS 814.01): « Les atteintes qui pourraient devenir nuisibles ou incommodantes seront réduites à titre préventif et assez tôt. » Voir aussi sur ce sujet le document de synthèse du groupe de travail interdépartemental "principe de précaution" d'août 2003 intitulé « Le principe de précaution en Suisse et au plan international ».

[43] Le 17 septembre 2014, un postulat Schwaab 14.3739 « Control by design: Renforcer les droits de propriété pour empêcher les connexions indésirables » a été déposé. Le Conseil fédéral propose son adoption. Les mesures de diligence envisagées dans ce chapitre pourraient concrétiser en partie le postulat, s'il était adopté par la suite.

- Principe du « Privacy by Design »: obligation pour les responsables du traitement de données (ou de leurs éventuels sous-traitants), dès la conception du traitement – pour autant qu'il porte sur des données personnelles – de tenir compte des exigences en matière de protection des données[44] et de prévoir des mesures de protection adéquates (p. ex : limitation au strict minimum des données traitées par l'application; sauvegarde décentralisée des données personnelles obtenues; intégration de mesures de sécurité techniques permettant de réduire le risque de traitements illicites des données). Pour l'application de cette obligation, il convient de prendre en considération notamment les risques que le traitement de données prévu présente pour la protection de la personnalité, les possibilités techniques, les standards reconnus ainsi que les coûts liés aux mesures. Dans ce cadre, on portera une attention particulière aux besoins de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.
- Principe du « Privacy by Default » : si les utilisateurs d'une application traitant des données ont la possibilité de choisir entre différents paramétrages, le réglage par défaut sera celui qui assure la plus grande protection des données personnelles [45]. Il convient de tenir compte tout spécialement du besoin de protection des mineurs et d'autres groupes de personnes particulièrement vulnérables.
- Documenter des processus de traitement des données : l'idée est que la protection des données ne peut être garantie que par celui qui sait quelles données il traite et comment ; cette condition ne peut être remplie que par une documentation adéquate lorsque la taille et la complexité d'une entreprise ainsi que la quantité de données traitées dépassent un certain niveau. Dans les grandes entreprises, une telle documentation doit retranscrire, avec une certaine précision, le traitement des données, les procédures et les opérations, l'organisation et les attributions ainsi que les moyens. Il existe des réglementations similaires dans d'autres textes législatifs (voir p. ex. art. 4 de l'ordonnance concernant la tenue et la conservation des livres de comptes ([Olico ; RS 221.431]). Cette documentation pourrait remplacer l'actuel registre des fichiers au sens de l'art. 11a LPD (cf. ch. 4.7) et peut-être aussi le règlement de traitement. Selon le groupe d'accompagnement, il n'est pas opportun de prévoir un droit d'accès à la documentation. Ce dernier ne contribuerait guère à la transparence, et la documentation en question contiendrait généralement aussi de nombreux secrets d'affaires, ainsi que des informations relatives à la sécurité. L'accès du PFPDT est réservé.
- Analyses d'impact: lorsque le traitement est susceptible de créer un risque accru d'atteinte à la personnalité, le responsable du traitement devrait procéder à des analyses de l'impact potentiel du traitement de données envisagé sur les droits des personnes concernées et fournir sur demande cette analyse à l'autorité de contrôle; là aussi, une attention particulière devrait être portée à l'impact sur les personnes mineures et les autres personnes vulnérables. On trouve des exemples d'analyses d'impact dans la législation

---

[44] On trouve un dispositif de réglementation analogue dans le domaine du droit de l'environnement et de l'aménagement du territoire, par exemple à l'art. 3 de l'ordonnance sur les chemins de fer (OCF ; RS 742.141.1): « Il y a lieu de tenir compte, dès la planification et l'établissement des projets, des exigences de l'aménagement du territoire, de la protection de l'environnement, ainsi que de celle de la nature et du paysage » (al. 1). « Il sera tenu compte de manière appropriée des besoins des handicapés » (al. 2).

[45] Le principe du « Privacy by Default » est étroitement lié au principe de la proportionnalité et à celui du « Privacy by Design ». Pour les auteurs de traitements de données, il peut en découler, dans certains cas, une obligation d'offrir aux utilisateurs un choix entre différents paramétrages du système.

suisse[46] (p. ex : art. 7 de l'ordonnance relative à l'étude de l'impact sur l'environnement[47], à l'art. 5 de la loi sur les produits chimiques[48] ou art. 5 de l'ordonnance de la Commission fédérale des maisons de jeu sur le blanchiment d'argent[49]).

- Obligation de signaler les violations des données à l'autorité de contrôle: à l'instar des réformes visées par le Conseil de l'Europe, le groupe d'accompagnement propose l'introduction d'une obligation de signaler les violations de données à caractère personnel (« data breaches »; pour la définition de ce terme, voir l'art. 4, al. 9, de la du projet de règlement UE[50]). L'art. 7, al. 2, du projet de modernisation de la Convention STE 108 stipule – en se fondant sur le droit de l'UE[51] – que l'autorité de contrôle (à tout le moins) doit être informée, sans retard injustifié, de violations de données qui pourraient porter gravement atteinte aux droits de la personnalité des personnes concernées. Pour déterminer quelles violations doivent être signalées, il convient de définir des critères dans la loi ou dans des règles de concrétisation (p. ex. des règles de bonnes pratiques ; voir ch. 4.1.2, let. b). *Une partie du groupe d'accompagnement* estime que l'obligation d'aviser l'autorité de contrôle ne doit être prévue que pour les cas où un grand nombre de personnes sont concernées par la violation de données. *D'autres membres du groupe* doutent en revanche qu'une telle réglementation ne satisfasse aux exigences du projet de modernisation de la Convention STE 108. Ils prônent dès lors l'établissement d'un catalogue de critères non exhaustif, qui prenne en compte notamment le type de données concernées et le risque concret pour les droits de la personnalité des personnes concernées. Outre l'obligation d'aviser l'autorité de contrôle, le groupe d'accompagnement propose d'obliger d'une manière générale les auteurs de traitements de données (ou leurs éventuels sous-traitants) à prendre des mesures appropriées pour limiter les dommages (p. ex : information des personnes concernées de la violation de données).
- Institution d'un conseiller à la protection des données : *une partie des membres du groupe d'accompagnement* propose de prévoir, dans les mesures de diligence, l'obligation pour les entreprises d'une certaine taille (p. ex. plus de 250 personnes en équivalent plein-temps), d'instituer un conseiller à la protection des données. Le Conseil fédéral pourrait étendre cette obligation aux entreprises plus petites qui présentent un risque accru. La notion de « risque accru » serait précisée dans le message, l'ordonnance ou encore des règles de bonnes pratiques ou des dispositions règlementaires (cf. ch. 4.1.2, let. b). Il s'agirait vraisemblablement des cas impliquant des données sensibles, des données per-

---

[46] Cf. aussi le rapport britannique suivant: <https://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment>.

[47] OEIE; RS 814.011.

[48] LChim; RS 813.1.

[49] OBA CFMJ; RS 955.021.

[50] En vertu de l'art. 4, al. 9, du projet de règlement UE une « violation de données à caractère personnel » est « une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière ».

[51] Concernant l'actuelle situation juridique, voir l'art. 4, al. 3, de la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) ainsi que le règlement (UE) N° 611/2013 du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE. *De lege ferenda* voir les art. 31 s. du projet de règlement UE et les art. 28 s. du projet de directive UE.

sonnelles concernant des mineurs ou d'autres personnes vulnérables, des données qui servent au profilage ou encore qui sont interconnectées à d'autres données (voir p. ex. art. 21 de l'ordonnance relative à la loi fédérale sur la protection des données [OLPD; RS 235.11]). À noter que les entreprises pourraient recourir à des conseillers externes afin notamment de bénéficier d'un savoir-faire qu'elles n'auraient pas autrement, sauf à engager une personne expressément, ou à former un employé dans ce but, ce qui pourrait constituer une charge financière importante. *Une autre partie du groupe d'accompagnement* estime qu'il ne faut pas mentionner cette obligation dans la loi, mais laisser aux règles de bonnes pratiques (cf. ch. 4.1.2 let. b) le soin de prévoir le ou les moyens les plus adéquats pour assurer un traitement des données respectueux des droits des personnes concernées selon les entreprises en cause (p. ex. la désignation d'un conseiller à la protection des données).

Au sein des organes fédéraux, il devrait impérativement y avoir un conseiller (« Datenschutzverantwortlicher ») au sens des art. 12a et 12b OLPD, qui exerce ses fonctions de façon indépendante et sans recevoir d'instructions[52] (cf. plus bas, ch. 4.9.4), à la place de l'actuel conseiller (« Berater für den Datenschutz ») selon l'art. 23 OLPD. Cette obligation doit s'appliquer au moins au niveau des départements. L'obligation pour les offices de disposer d'un conseiller à la protection des données pourrait dépendre du type et de la quantité de données traitées.

– Aux fins d'améliorer la prise en compte de la protection des données, en particulier dans les projets informatiques, une *partie du groupe d'accompagnement* propose d'examiner l'opportunité d'obliger les organes fédéraux à mettre en place dans les départements des systèmes de gestion de la protection des données et de la sécurité informatique. D'autres devoirs de diligence (p. ex. le principe du « Privacy by Design » ou l'obligation d'évaluer l'impact sur la protection des données) pourraient toutefois déjà suffire à imposer une telle mesure ; ce point devrait plutôt être réglé au niveau ordonnance.

4.3.3 Consentement

Pour ce qui est des exigences liées au consentement, traitées actuellement dans les principes (art. 4, al. 5, LPD), le groupe d'accompagnement propose, pour autant que cette solution soit compatible avec le projet de modernisation de la Convention STE 108, de maintenir le système en vigueur. *Le groupe d'accompagnement* estime par ailleurs qu'il convient de prendre des mesures pour améliorer la qualité du consentement. En effet, à l'heure actuelle, en raison d'un défaut d'information ou d'un processus informatif trop complexe, mais aussi parfois d'un défaut de curiosité, les personnes concernées consentent à des traitements qu'elles ne connaissent pas, ne comprennent pas, qui ne les intéressent pas, ou parfois même qu'elles ne choisissent pas. Un renforcement du devoir d'information (ch. 4.3.1), le choix systématique de technologies respectueuses des droits des particuliers (ch. 4.3.2), ou encore une sensibilisation accrue par l'autorité de contrôle (ch. 4.10.2, let. d) permettraient d'améliorer la situation. Ces mesures pourraient être concrétisées par des règles de bonnes pratiques, voire des réglementations contraignantes (ch. 4.1.2, let. b).

4.3.4 Autres principes

Les autres principes contenus dans les actuels art. 4 et 5, al. 1, et 7 LPD devraient être

---

[52] Les tâches et la position du conseiller à la protection des données (Datenschutzverantwortlicher) sont expliquées sur le site du PFPDT, à l'adresse suivante : http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr.

maintenus dans la mesure où ils ont fait leurs preuves.

4.4 Droits des personnes concernées

4.4.1 Introduction

La protection des droits individuels, parallèlement à la surveillance par l'autorité de contrôle, joue un rôle central dans la garantie du respect du droit de la protection des données. Comme cela a été expliqué plus haut, *une partie du groupe d'accompagnement* estime que les possibilités de renforcer la protection des droits individuels par le biais des dispositions légales sont minces (voir ch. 4.1.2, let. a, ainsi que ch. 4.8.3 et 4.9.5). Quoi qu'il en soit, l'évaluation de la LPD a révélé que les personnes concernées font rarement valoir leurs droits à l'encontre des auteurs de traitements de données, surtout dans le secteur privé. Cette retenue pourrait résider dans une méconnaissance des prétentions existantes et des procédures applicables [53]. Le groupe d'accompagnement propose par conséquent :

- d'améliorer la structure et la lisibilité de la LPD afin que les personnes concernées voient clairement quels sont leurs droits (cf. ch.4.4.2) ; et
- de renforcer, au moins ponctuellement, les droits des personnes concernées (cf. ch. 4.4.3 ss) ainsi que les procédures de mise en œuvre (voir ch. 4.8.3, let. b, et 4.9.5, let. c), en particulier dans les domaines où des lacunes subsistent en comparaison des travaux de réforme de la protection des données entrepris par le Conseil de l'Europe.

4.4.2 Catalogue des prétentions

Les dispositions concernant les droits des personnes concernées sont actuellement réparties dans différents articles et sections de la loi (le droit à la rectification est ainsi réglé à l'art. 5, al. 2, à l'art. 15, al. 1, et à l'art. 25, al. 3, let. a, LPD). Les prétentions sont en partie formulées aussi sous forme de moyens procéduraux, qui ne sont pas toujours délimités nettement les uns par rapport aux autres, mais se recoupent en partie. Il est par conséquent difficile pour les intéressés de connaître précisément leurs droits. Le groupe d'accompagnement estime également que la structure de l'actuelle LPD ne fait pas clairement ressortir que les personnes concernées peuvent (et devraient) faire valoir directement leurs droits (d'accès, d'opposition, à la rectification, à l'effacement, de blocage etc.) auprès des auteurs de traitements et qu'il n'est pas nécessaire d'introduire d'abord une action en justice. Le groupe d'accompagnement propose donc de dresser un catalogue des prétentions que peuvent faire valoir les personnes concernées, comme l'ont fait du reste le Conseil de l'Europe[54] et l'UE[55] dans leurs projets de réforme, ou comme c'est le cas à l'art. 25 LPD (prétentions et procédure en rapport avec le traitement de données par des organes fédéraux). Il serait ainsi plus facile pour les personnes concernées de savoir quels droits elles peuvent faire valoir à l'encontre de qui et, cas échéant, d'agir judiciairement. Les prétentions devraient autant que possible être les mêmes pour les secteurs public et privé. En font notamment partie :

- le droit d'accès (« Auskunftsrecht »; cf. plus bas, ch. 4.4.3) ;
- le droit à la rectification de données personnelles erronées (« Berichtigung »; cf. plus bas, ch. 4.4.4);

---

[53] Voir le rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données, FF 2012 255, 260 s.

[54] Cf. l'art. 8 du projet de modernisation de la Convention STE 108.

[55] Cf. le chapitre III du projet de règlement et du projet de directive UE.

- le droit à l'effacement (« Löschung ») ou le droit à la destruction (« Vernichtung ») de données personnelles ayant fait l'objet d'un traitement illicite (cf. plus bas, ch. 4.4.5);
- le droit de faire interdire un traitement illicite ou la communication de données personnelles à des tiers (« Sperrung ») ;
- le droit de faire mentionner le caractère litigieux (« Bestreitungsvermerk »), lorsque ni l'exactitude ni l'inexactitude d'une donnée personnelle ne peut être établie ;
- le droit d'opposition (« Widerspruch ») à un traitement de données sans motif justificatif ;
- le droit pour la personne concernée de ne pas être soumise à une décision fondée sur un traitement purement automatique de données qui la touche de manière substantielle, sans qu'elle ne puisse faire valoir son point de vue (cf. ch. 4.4.6).

Ce catalogue des droits doit permettre aux intéressés de mieux comprendre la loi sur la protection des données. En revanche, l'actuel système d'exercice des droits (p. ex. s'agissant de la légitimation active et passive) doit pour l'essentiel rester inchangé sur le plan matériel. Les prétentions en réparation (dommages-intérêts, réparation pour tort moral, remise de gain) doivent continuer à obéir aux conditions générales du droit de responsabilité civile et publique (voir pour l'ensemble, voir ch. 4.8.3 et 4.9.5).

Différentes mesures sont proposées ci-après pour renforcer les droits des personnes concernées en matière de protection des données.

4.4.3 Droit d'accès

Le groupe d'accompagnement propose de compléter les dispositions sur le droit d'accès de manière à améliorer la transparence des traitements. Sur demande, et comme le prévoit le projet de modernisation de la Convention STE 108, le responsable du traitement devrait également communiquer à la personne concernée la durée de conservation ainsi que le raisonnement qui sous-tend le traitement de données dont les résultats lui sont appliqués (cf. art. 8, let. c et d, du projet de modernisation de la Convention STE 108).

De plus en plus souvent, les données personnelles sont structurées en fonction des applications pour établir des profils éphémères. Il n'existe alors pas de fichier permanent, ce qui rend le droit d'accès inopérant. Le groupe d'accompagnement est conscient de ce problème. *Une partie du groupe* estime qu'il doit être résolu par le biais du devoir d'information (voir ch. 4.3.1) et non par le biais du droit d'accès.

Il faut en outre examiner l'opportunité de concrétiser les modalités du droit d'accès selon l'art. 8, al. 5, LPD. Il pourrait par exemple être arrêté que la charge (coûts compris) que représente la fourniture des renseignements doit être proportionnelle par rapport au but du droit d'accès (p. ex. consultation des informations sur place à la place d'une notification par écrit).

L'art. 8, al. 6, LPD doit être revu de manière à ce qu'il ressorte clairement de sa formulation ou de sa structure qu'il est possible de renoncer par avance à la fourniture de renseignements par écrit, pour autant que la consultation soit dûment assurée.

Une partie du groupe d'accompagnement souhaite introduire de manière générale une pesée des intérêts pour l'exercice du droit d'accès, lorsque les données sont archivées ou stockées en raison d'une obligation légale. Il s'agira de vérifier si cette solution est compatible avec le projet de modernisation de la Convention STE 108, ce dont doutent certains membres du groupe.

Pour ce qui est des restrictions au droit d'accès, *une partie du groupe d'accompagnement* estime qu'il convient de supprimer la condition de la non-communication des données à un

tiers qui figure à l'actuel art. 9, al. 4, LPD, dans la mesure où ce critère n'a aucun lien avec les intérêts prépondérants du maître de fichier. La loi contiendrait plutôt une liste exemplative de ce qui est susceptible de constituer un tel intérêt. Il s'agirait par exemple de la sauvegarde d'intérêts commerciaux ou industriels, de l'atteinte grave aux intérêts de la source d'information, de la non-révélation d'une stratégie judiciaire dans une procédure qui opposerait le responsable du traitement à la personne concernée ou des demandes d'accès chicanières. *Une autre partie du groupe d'accompagnement* estime qu'une telle option affaiblirait la position de la personne concernée et propose de conserver la condition de l'absence de communication des données à un tiers. La loi ou l'ordonnance prévoiraient alors des exceptions, dans le respect de l'art. 9 du projet de modernisation de la Convention STE 108.

Il faut enfin réfléchir à l'opportunité d'insérer dans la loi la teneur de l'actuel art. 1, al. 7, OLPD, qui concerne la consultation des données d'une personne décédée. Cette disposition est en effet dépourvue de base légale, dans la mesure où la LPD ne régit pas les données des personnes décédées.

4.4.4 Droit à la rectification

Le droit à la rectification doit être complété de la manière suivante : si une personne responsable du traitement de données reçoit une demande de rectification de données et la considère comme justifiée, elle doit en informer les éventuels destinataires dont elle a connaissance afin que ces informations soient également corrigées en aval. Cette exigence ne doit pas être absolue ; il est possible de prévoir des restrictions (p. ex. si l'information aux destinataires est impossible ou disproportionnée par rapport à l'importance de l'erreur).

4.4.5 Droit à l'effacement

Ce droit existe aujourd'hui déjà; la personne dont les données sont traitées en violation de la LPD peut demander à l'auteur du traitement et au juge, sous réserve de l'existence d'un motif justificatif, que ses données soient effacées ou retirées d'un site internet par exemple, mais aussi d'un programme informatique (cf. art. 15 et 25 LPD). Il s'agit ici plus de mentionner expressément ce droit à titre symbolique, dans la perspective de faciliter la compréhension de la loi pour les personnes concernées. Cette mention expresse ne changera rien au plan matériel. Il sera par exemple toujours possible de traiter des données contre la volonté des personnes concernées en présence d'intérêts prépondérants, tels l'intérêt des médias ou la recherche historique[56].

Le groupe d'accompagnement propose d'utiliser les termes de « droit à l'effacement » plutôt que de « droit à l'oubli », cela principalement pour coller à la terminologie du Conseil de l'Europe (art. 8, let. e, du projet de modernisation de la Convention STE 108). Le droit à l'effacement sera renforcé par l'introduction des mesures de diligence (ch. 4.3.2), le renforcement du droit d'accès (ch. 4.4.3) et ses modalités précisées dans des règles de bonnes pratiques ou des règles contraignantes (ch. 4.1.2, let. b).

Le groupe d'accompagnement estime qu'avec ces mesures, il aura réalisé le postulat Schwaab 12.3152 « Droit à l'oubli numérique »[57] et partiellement réalisé le postulat Recordon 13.3989 « Violations de la personnalité dues au progrès des techniques de l'information et de la communication ».

---

[56] Voir pour une décision en ce sens l'arrêt de la CEDH n° 33846/07 «Wegrzynowski et Smolczewski c. Pologne» du 16 juillet 2013.

[57] Le postulat Schwaab 12.3152 du 14 mars 2012 a été adopté par le Conseil national le 15 juin 2012.

4.4.6 Décisions individuelles automatisées

Les nouvelles technologies de l'information et de la communication, font que de plus en plus souvent, des décisions produisant des effets juridiques pour les personnes concernées ou pouvant les affecter de manière significative sont prises dans le cadre de procédures automatisées, voire sur la base de profils reposant sur des données statistiques et des calculs (profilage). *Une majorité du groupe d'accompagnement* estime qu'il y a un besoin accru de protection en particulier lorsque de telles procédures de décision portent sur les caractéristiques d'une personne, par exemple sa solvabilité[58], sa fiabilité, son comportement ou des risques spécifiques[59]. L'UE s'est dotée il y a quelque temps déjà de prescriptions sur l'admissibilité de décisions individuelles automatisées[60]. La mise en œuvre de ces dispositions ne pose pas, à notre connaissance, de problème dans les États membres.

La majorité du groupe d'accompagnement propose dès lors de conférer à toute personne le droit – en conformité avec l'art. 8, let. a, du projet de modernisation de la Convention STE 108[61] – de ne pas être soumise à une décision fondée sur un traitement purement automatique et qui l'affecterait de manière significative, sans que son point de vue ne soit pris en compte, avant ou après la décision automatique. Le but est d'empêcher que l'évaluation d'aspects de la personnalité se fasse de façon entièrement automatique, sans intervention humaine et sans que la personne concernée n'apprenne comment cette décision a été prise. Celle-là doit avoir la possiblité de faire valoir ses arguments et d'éventuels faits qui n'auraient pas été pris en compte dans l'évaluation afin que la dimension humaine soit intégrée en dépit du traitement automatisé des données.

Dans ce contexte, il faut encore examiner plus précisément quelles procédures doivent être qualifiées de décisions individuelles automatisées au sens décrit ci-dessus. Le retrait d'argent à un guichet automatique ou l'envoi de prospectus à une série de personnes déterminées par ordinateur ne devraient par exemple, pas être soumis à la réglementation proposée, comme c'est le cas en droit européen. Par ailleurs, il ne doit pas s'agir d'un droit absolu, des exceptions légales pouvant être prévues. Il convient de préciser que la réglementation proposée ne doit pas empiéter sur la liberté de se déterminer et la liberté contractuelle (pas d'obligation de contracter), ni entraîner une obligation de motiver les décisions individuelles automatisées.

Une minorité du groupe d'accompagnement souhaite que ce droit soit complété par un droit de s'opposer au profilage prédictif automatisé, sous réserve d'exceptions, comme le prévoit l'art. 20 du projet de règlement UE. Les profils qui en résultent peuvent en effet entraîner des erreurs d'appréciation ou des discriminations.

---

[58] Le profilage est utilisé dans le secteur bancaire par exemple en rapport avec l'octroi de crédits et l'analyse de risque de clients, présents ou futurs (credit-scoring).

[59] Cf. le message du Conseil fédéral du 19 février 2003 relatif à la révision de la loi sur la protection des données (LPD), FF 2003 1915, 1945: ce serait le cas par exemple si une assurance responsabilité civile rangeait une conductrice possédant une petite voiture dans une classe de risque moins élevée qu'un conducteur qui a une voiture de sport.

[60] Voir en particulier l'art. 15 de la directive 95/46/CE et l'art. 7 de la décision-cadre 2008/977/JAI. Le projet de règlement UE prévoit à l'art. 20 des dispositions relatives aux « mesures fondées sur le profilage », tout comme l'art. 9 du projet de directive UE.

[61] Art. 8, let. a, du projet de modernisation de la Convention STE 108 : « Toute personne doit pouvoir: (...) ne pas être soumise à une décision l'affectant de manière significative, qui serait prise sur le seul fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte ».

Une autre minorité du groupe d'accompagnement s'oppose à l'introduction d'un tel droit.

Concernant le droit de renseignement sur la structure logique du traitement des données, voir plus haut ch. 4.4.3.

4.4.7 Droit à la portabilité des données

Une partie du groupe d'accompagnement propose que l'on introduise dans la LPD un droit à la portabilité des données pour les personnes concernées, comme le prévoit le projet de règlement UE (art. 18 du projet de la Commission). *Une autre partie du groupe d'accompagnement* est d'avis que ce droit relève plus du droit de la concurrence ou du droit des médias[62] que de la protection des données et estime ainsi que l'on ne doit pas l'introduire dans la LPD. Le groupe d'accompagnement propose de suivre les travaux au plan européen, et de réexaminer la question si ce droit devait être maintenu dans le projet de règlement UE.

4.5 Communication transfrontière de données

Pour l'essentiel, les règles contenues dans l'actuel art. 6 LPD ont fait leurs preuves. Le groupe d'accompagnement prévoit toutefois quelques modifications.

L'art. 6, al. 2, let. d, LPD — qui prévoit que malgré l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, des données personnelles peuvent être communiquées à l'étranger si la communication est, en l'espèce, indispensable à l'exercice ou la défense d'un droit en justice — pose un problème d'interprétation. Le texte allemand diverge des textes français et italien. Alors que ces derniers parlent de « la constatation, l'exercice ou la défense d'un droit en justice » et de « accetertare, esercitare o far valere un diritto in giustizia » respectivement, la version allemande parle de « Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht ».

Certains auteurs considèrent que l'exception doit être interprétée largement, la procédure ne devant pas forcément se dérouler devant un tribunal[63]. *Une partie du groupe d'accompagnement* soutient cette opinion, et estime qu'il convient d'adapter le texte allemand aux textes français et italien. *Une autre partie du groupe* estime au contraire que les exceptions, sous peine de vider la protection des données de son contenu en cas d'échange de données avec l'étranger, ne doivent concerner que les procédures devant un tribunal et préconise ainsi d'adapter les textes latins à l'allemand.

Le groupe d'accompagnement propose au surplus d'étendre l'exception de l'actuel art. 6, al. 2, let. e, LPD à la vie et à l'intégrité corporelle de tiers. Il est en effet possible que des données personnelles de la personne concernée soient indispensables à la sauvegarde de tels intérêts mais que celle-là ne soit pas atteignable (p. ex. : une adresse, un numéro de téléphone, ou des données médicales).

---

[62] Pour ce qui est de la problématique de la portabilité des données dans le cadre de l'utilisation des médias sociaux, et du besoin de légiférer dans ce domaine, voir le rapport du Conseil fédéral «Cadre légal pour les médias sociaux : Rapport en réponse au postulat Amherd 11.3912 du 29 septembre 2011», pp. 37 s. et 78.

[63] MEIER, Protection des données, Fondements, principes généraux et droit privé, Berne 2011, N 1375, pour qui il s'agit de « toute procédure pendante devant un organe étatique (y compris de juridiction administrative interne) ou reconnu par l'Etat »; MAURER-LAMBROU/STEINER, in: Maurer-Lambrou/Blechta (édit.), Datenschutzgesetz – Öffentlichkeitsgesetz, 3e éd., Bâle 2014, art. 6 LPD, N 33, qui estime qu'il s'agit de « jede Instanz mit Rechtsprechungsfunktion ».

En lien avec l'art. 6, al. 3, LDP, on pourrait prévoir que les garanties mentionnées à l'art. 6, al. 2, let. a, et les règles de protection des données mentionnées à l'art. 6, al. 2, let. g, LPD valent comme protection adéquate lorsque l'autorité de contrôle les a approuvées. L'obtention de l'approbation de l'autorité de contrôle serait facultative. Les entreprises qui le souhaitent pourraient soumettre leurs « Binding Corporate Rules » (BCR)[64]. Les conditions à remplir ainsi que la procédure pourraient être prévues par des règles de bonnes pratiques ou des règles contraignantes (cf. ch. 4.1.2, let. b).

Il convient en outre d'adapter la formulation allemande de la phrase introductive de l'art. 6, al. 2 à la version française (adjonction après « wenn » de « eine der folgenden Bedingungen erfüllt ist »).

Enfin, il faudrait préciser que l'adéquation de la protection des données dans le cadre de la communication transfrontière de données selon l'art. 6, al. 1, LPD ne suppose pas la protection des données de personnes morales (cf. ch. 4.2.1, let. b).

4.6 Procédure de certification

La possibilité de certification selon l'art. 11 LPD doit être maintenue. La formulation de cette disposition mérite cependant d'être revue. S'agissant de la certification de produits, dont la mise en oeuvre a présenté certaines difficultés, le mandat donnée à l'autorité de contrôle d'édicter des directives (voir art. 5, al. 3, de l'ordonnance sur les certifications en matière de protection des données [OCPD; RS 235.13]) doit être transformé en une disposition potestative (Kann-Vorschrift). L'autorité de contrôle jouirait ainsi d'une plus grande marge de manœuvre. Il faut en outre examiner s'il convient d'introduire une certification pour les prestations de service, en tenant compte des développements au niveau européen. La certification devrait de manière générale demeurer facultative. La possibilité de prévoir une certification obligatoire dans des lois spéciales serait maintenue (voir p. ex. art. 59a de l'ordonnance sur l'assurance-maladie [OAMal; RS 832.102]).

4.7 Registre des fichiers

Le groupe d'accompagnement propose de renoncer à la tenue d'un registre des fichiers telle qu'elle est prévue à l'art. 11a LPD, car elle constitue une lourdeur bureaucratique qui a peu d'utilité pratique dans le secteur privé, d'autant que la loi actuelle prévoit déjà des exceptions à l'obligation d'annoncer les fichiers. En lieu et place, le groupe d'accompagnement propose d'introduire, dans les mesures de diligence, un devoir de documenter de manière adéquate les traitements de données (voir ch. 4.3.2). La tenue du registre pourrait être maintenue pour le secteur de l'administration fédérale.

4.8 Dispositions particulières relatives au traitement de données personnelles par des particuliers

4.8.1 Conception de la réglementation

Selon la conception actuelle de la LPD, la protection des données de droit privé complète et concrétise la protection de la personnalité du code civil. Les droits de la personnalité sont indissociables de la personne concernée. Il s'agit de droits absolus, hautement personnels et incessibles. La loi mentionne de façon exemplative les cas dans lesquels un traitement de données constitue une atteinte à la personnalité et indique quels motifs peuvent justifier une

[64] Les « Binding Corporate Rules » désignent, dans l'UE, un code de conduite qui définit la politique interne d'un groupe en matière de transferts de données personnelles hors de l'UE.

telle atteinte. Ce système doit être maintenu. Il n'est pas prévu actuellement de passer à un modèle où les données personnelles seraient protégées par l'attribution de droits de propriété (c.à-d. un droit des disposer et d'utiliser des données personnelles[65]). En effet, le groupe d'accompagnement considère que l'opportunité d'un tel changement de système n'est pas établi. Un droit de maîtrise absolu de chacun sur ses données serait en désaccord flagrant avec d'autres intérêts, tels que la liberté d'opinion et d'information. Le groupe d'accompagnement propose en lieu et place une série d'autres mesures afin d'assurer aux personnes concernées une meilleure maîtrise de leurs données (cf. p. ex. les réglementations proposées pour renforcer l'obligation d'informer [ch. 4.3.1], pour les principes du « Privacy by Design » et du « Privacy by Default » [ch. 4.3.2] ainsi que pour les tâches de l'autorité de contrôle visant à sensibiliser la population aux questions de protection des données [ch. 4.10.2, let. d]).

4.8.2 Atteintes à la personnalité et motifs justificatifs

Les art. 12 et 13 LPD, qui arrêtent les conditions auxquelles les traitements de données personnelles par des privés sont licites, doivent être maintenus. Le groupe d'accompagnement propose toutefois les modifications suivantes :

Répartition du fardeau de la preuve : selon les règles générales en vigueur (art. 8 CC), la personne concernée doit en principe apporter la preuve de l'atteinte à la personnalité, tandis que l'auteur du traitement doit prouver l'existence d'un motif justificatif. La personne concernée pourrait rencontrer des difficultés à apporter cette preuve vu la complexité croissante des méthodes de traitement des données que permettent les développements technologiques. *La majorité du groupe d'accompagnement* souhaite tenir compte de cette évolution et alléger le fardeau de la preuve. À cet effet, elle propose un renversement du fardeau de la preuve, sur l'exemple de l'art. 13a. al. 1, LCD[66]. Le juge pourrait exiger de l'auteur d'un traitement de données qu'il prouve, dans le cas particulier, que le traitement est conforme aux dispositions sur la protection des données, si, compte tenu des intérêts légitimes des parties à la procédure, une telle exigence paraît appropriée (concernant la présomption légale de la régularité d'un traitement de données lorsque les règles de bonnes pratiques sont respectées, voir plus haut ch. 4.1.2, let. b). Une telle exigence pourrait s'appliquer lorsque l'administration des preuves est particulièrement difficile pour la personne concernée, parce que les faits à prouver sont dans la sphère d'influence de l'auteur du traitement (p. ex. en

---

[65] Dans la doctrine, la question de l'introduction de droits de maîtrise ou de droits similaires est discutée depuis quelques temps en lien avec l'exigence d'une amélioration du contrôle sur les données. Chaque personne pourrait avoir un droit absolu et illimité de disposer de ses données. Les avantages avancés pour ce système sont notamment un meilleur contrôle et la participation de chacun au produit financier résultant de l'utilisation de ses données. La critique, elle, concerne la maîtrise absolue des données, qui pourrait déboucher sur une monopolisation du savoir et de l'information. En outre, il est précisé que même dans un tel système il n'y aurait guère de partenaires contractuels égaux dans le « commerce des données ». Voir à ce propos par exemple FLÜCKIGER, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, pp. 837–864 ou SCHUNCK, Propertisierung von Personendaten?, digma 2013, pp. 66–72. Dans ce contexte, il faut aussi prendre en considération l'initiative parlementaire Derder 14.434 « Protéger l'identité numérique des citoyens », qui vise à inscrire à l'art. 13, al. 2, Cst. que « Ces données sont la propriété de la personne […] ». Cette initiative n'a pas encore été traitée.

[66] Art. 13a, al. 1, LCD: « Le juge peut exiger que l'annonceur apporte des preuves concernant l'exactitude matérielle des données de fait contenues dans la publicité si, compte tenu des intérêts légitimes de l'annonceur et de toute autre partie à la procédure, une telle exigence paraît appropriée en l'espèce. »

rapport avec le respect du devoir de diligence selon le ch. 4.3.2). *Une minorité du groupe d'accompagnement* estime par contre qu'une telle réglementation n'est pas nécessaire, dans la mesure où l'administration des preuves ne constitue pas un problème central dans la pratique. En cas de difficultés concernant la preuve de faits qui sont du ressort de l'auteur du traitement, le juge civil en tient compte dans le cadre de l'obligation de collaborer et de l'appréciation des preuves.

Atteintes à la personnalité : *une partie du groupe d'accompagnement* estime qu'il faut réintroduire explicitement dans l'art. 12, al. 2, let. a, LPD – qui stipule qu'un traitement de données personnelles fait en violation des principes généraux définis constitue toujours une atteinte à la personnalité – la possibilité de faire valoir des motifs justificatifs. La réserve des motifs justificatifs a en effet été rayée de l'art. 12, al. 2, let.a, LPD lors de la révision de la loi du 24 mars 2006[67], à la différence des let. b et c du même article. Pour motiver cette proposition de modification (p. ex. dans le commentaire d'un éventuel projet de révision), il faut souligner que la doctrine majoritaire et le Tribunal fédéral partent du principe qu'une justification du traitement de données personnelles en violation des principes généraux n'est pas exclue d'une manière générale, mais que le motif justificatif ne peut être admis qu'avec la plus grande retenue. *D'autres membres du groupe d'accompagnement* tiennent en revanche à conserver la formulation actuelle. Ils estiment qu'il n'est pas nécessaire de modifier l'art. 12, al. 2, let. a, LPD, vu que le Tribunal fédéral admet, dans certains cas, des motifs justificatifs même avec la teneur actuelle de la disposition.

Motifs justificatifs : le groupe d'accompagnement propose de compléter l'énumération exemplative de l'art. 12, al. 2, LPD, en ajoutant d'autres situations dans lesquelles le traitement de données peut être justifié par des intérêts privés prépondérants, à savoir :

- Traitement de données de personnes morales dans le cadre de leur activité commerciale (p. ex. lorsqu'une personne traite des données concernant sa clientèle et ses fournisseurs ou lorsqu'il s'agit de l'exécution d'un contrat avec ces derniers ; cf. ch. 4.2.1, let. b). *Une partie du groupe d'accompagnement* propose d'étendre ce motif justificatif aux entreprises qui n'ont pas la qualité de personne morale (p. ex. des sociétés simples ou des communautés d'héritiers). Les conséquences juridiques qu'aurait une telle extension doivent encore faire l'objet d'un examen approfondi.
- Traitement de données personnelles en vue de procédures judiciaires ou administratives (en Suisse ou à l'étranger) (par analogie à l'art. 6, al. 2, let. d, lorsque le traitement est indispensable à la constatation, à l'exercice ou à la défense d'un droit). Le groupe n'est toutefois *pas unanime* sur l'opportunité d'inclure aussi les procédures administratives ; cf. ch. 4.5.
- Conclusion ou exécution d'un contrat comme motif justificatif selon l'art. 13, al. 2, let. a, LPD : *une partie du groupe d'accompagnement* estime qu'il faut examiner si les exigences pour justifier un traitement de données ne devraient pas être assouplies, en particulier si le motif justificatif de l'art. 13, al. 2, let. a ne pourrait pas être étendu à des situations où le contrat n'a pas été conclu formellement avec la personne concernée, mais où celle-ci en bénéficie (p. ex. dans le cadre d'un contrat de travail)[68]. Le groupe

[67] Cf. RO 2007 4983.

[68] Concernant la communication de données personnelles à l'étranger ou les échanges entre services internationaux ou intergouvernementaux, la loi allemande sur la protection des données (Bundesdatenschutzgesetz ; BDSG) arrête par exemple à son § 4c, al. 1, ch. 3, que dans le cadre d'activités qui entrent, partiellement ou intégralement, dans le champ d'application du droit de la Communauté européenne, une communication de données

d'accompagnement a décidé de laisser cette question ouverte[69],[70].

- Une *partie du groupe d'accompagnement* souhaite introduire un autre motif justificatif, à savoir le traitement de données personnelles à des fins d'archivage ou de sécurité.

4.8.3 Prétentions et procédures

a) Prétentions

Comme mentionné aux ch. 4.4.1 et 4.4.2, il est prévu d'adapter la structure et la clarté de la LPD afin qu'il soit plus aisé pour les personnes concernées de voir quelles sont leurs prétentions. Il doit notamment ressortir plus clairement de la loi que les personnes concernées peuvent dans un premier temps faire valoir leurs droits auprès des auteurs privés de traitements de données seuls et directement, sans devoir intenter une action en justice. À cet effet, il est prévu notamment de dresser un catalogue des prétentions des personnes concernées, comprenant notamment les droits d'accès, de contestation, de rectification ou d'effacement.

Une majorité du groupe d'accompagnement est en revanche d'avis qu'il ne faut rien changer matériellement à l'actuel système d'exercice des droits (p. ex. s'agissant de la légitimation active et passive). De même, les prétentions en dommages-intérêts ou en réparation pour tort moral doivent continuer à obéir aux règles générales du droit de la responsabilité civile. S'agissant de la remise de gain, les dispositions du CO relatives à la gestion d'affaires sans mandat[71] restent applicables telles quelles (cf. art. 15, al. 1, LPD, en relation avec l'art. 28a, al. 3, CC et les art. 41 ss, 49 et 423 du code des obligations [CO; RS 220]). *Quelques membres du groupe d'accompagnement* proposent en revanche de supprimer la relation avec les dispositions du CC et du CO, et de régler les prétentions qui y sont régies dans la LPD même.

Le groupe d'accompagnement est partagé sur l'opportunité d'introduire une responsabilité objective pour les actions en réparation. Certains estiment qu'il y a dans le domaine de la protection des données trop peu de cas de dommages financiers ou de tort moral pour justifier l'introduction d'une telle responsabilité. D'autres estiment en revanche que le peu d'affaires portées devant les tribunaux ne permet pas de tirer de conclusions quant à l'importance et à la fréquence des cas dans lesquels une indemnité serait justifiée. Ils estiment dès lors que l'introduction d'une responsabilité objective permettrait aux particuliers de faire valoir leurs droits plus facilement. Certains préconisent même d'instituer un système d'indemnisation forfaitaire sur le modèle de l'art. 336a CO pour le licenciement abusif.

---

personnelles à des services autres que ceux qui sont énumérés au § 4, al. 1, est admissible, même si le niveau de protection requis n'est pas garanti, dans la mesure où la communication des données est nécessaire pour conclure ou exécuter un contrat que le service responsable a conclu ou va conclure avec un tiers dans l'intérêt de la personne concernée (traduction non officielle).

[69] Si l'art. 13, al. 2. let. a, LPD devait être modifié, il faudrait également adapter l'art. 6, al. 2. let. c, LPD pour des raisons de cohérence.

[70] Concernant la situation juridique dans l'UE, voir l'art. 6, ch. 1, let. b, du projet de règlement UE: « Le traitement de données à caractère personnel n'est licite que si et dans la mesure où l'une au moins des situations suivantes s'applique: […] le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci » (similaire à l'art. 7, let. b, de la directive 95/46/CE).

[71] Lors des futurs travaux de révision de la LPD, il conviendra d'étudier plus en détail si le renvoi à l'art. 423 CO est un renvoi aux effets juridiques (Rechtsfolgeverweis) ou un renvoi à la cause (Rechtsgrundverweis).

b) Dispositions de procédure

L'évaluation de la LPD a montré que les personnes concernées font rarement valoir leur prétentions. Les raisons avancées dans le rapport d'évaluation du Conseil fédéral sont notamment une relative méconnaissance de ces prétentions et de leur mise en oeuvre (cf. ch. 4.4.1). Il est également possible que les personnes concernées considèrent que l'effort à fournir pour intenter une action est trop important par rapport au bénéfice diffus et incertain d'une victoire judiciaire[72]. Pour ces raisons, le groupe d'accompagnement a étudié différents modèles permettant aux individus d'obtenir la mise en œuvre de leurs droits, tels le renforcement de la position procédurale des personnes concernées dans l'exercice du droit d'opposition, l'introduction de la maxime inquisitoire ou l'application de la procédure simplifiée au sens des art. 243 ss. du code de procédure civile (CPC; RS 272) pour toutes les actions concernant la protection des données[73], l'allégement des frais de procédure ou encore le développement d'instruments d'exercice collectif des droits, sous la forme d'actions des organisations, d'actions de groupe, ou d'actions modèles ou test.

Une *partie du groupe d'accompagnement* estime que l'effet des mesures envisagées ci-dessus serait plutôt faible, c'est-à-dire que les modalités d'exercice des droits des personnes concernées ne seraient que peu facilitées. Ces mesures sont aussi considérées comme problématiques, car elles risquent de rompre le lien entre la LPD et la protection de la personnalité générale du code civil, ce qui créerait deux systèmes distincts dans le droit civil suisse pour garantir la protection de la personnalité. Cette partie du groupe d'accompagnement est donc d'avis que, pour garantir le respect des dispositions de protection des données par les auteurs de traitements privés, il faut avant tout renforcer la surveillance et étendre en conséquences les compétences de l'autorité de contrôle (ch. 4.10.2).

Une autre partie du groupe d'accompagnement est en revanche d'avis qu'il faut aussi proposer des mesures importantes pour renforcer la position des particuliers, car la protection des droits individuels est un problème avéré selon le rapport d'évaluation. Il est par ailleurs selon elle risqué de ne proposer que le renforcement des pouvoirs de l'autorité de contrôle, qui nécessitera des ressources importantes, dans le contexte actuel de restrictions budgétaires imposées par le Parlement.

Pour améliorer, au moins ponctuellement, la protection juridique des personnes concernées, les mesures suivantes sont proposées :

Allégement des frais de procédure : les avis du groupe d'accompagnement sur cette question sont partagés. Certains estiment que ce ne sont pas les frais de justice eux-mêmes, mais bien plus les avances de frais et les dépens potentiels qui dissuadent les parties de faire usage des voies de droit. *Une partie du groupe d'accompagnement* propose de fixer une fourchette nettement réduite pour les frais judiciaires dans les litiges en matière de protection des données, en prenant modèle sur l'art. 65, al. 4 et 5, de la loi sur le Tribunal fédéral (LTF; RS 173.110)[74]. Il convient en outre d'examiner quelles mesures pourraient être

---

[72] Cf. le rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données, FFI 2012 255, 261 s.

[73] *De lege lata*, la procédure simplifiée n'est applicable qu'aux actions en exécution du droit d'accès selon l'art. 8 LPD (art. 15, al. 4, LPD, en relation avec art. 243, al. 2, let. d, CPC), pour autant qu'il ne s'agisse pas d'une affaire patrimoniale dont la valeur litigieuse ne dépasse pas 30 000 francs (art. 243, al. 1, CPC). Pour le reste, la procédure ordinaire selon les art. 219 ss CPC est applicable à toutes les autres actions en matière de protection des données.

[74] La teneur de l'art. 65, al. 4 et 5, LTF est la suivante : « Il [le montant des frais judiciaires] est fixé entre 200 et 1000 francs, indépendamment de la valeur litigieuse, dans les affaires qui concernent: a. des prestations

prises concernant les avances de frais afin de faciliter l'accès à la justice. *Une autre partie du groupe d'accompagnement* se prononce contre une réglementation spéciale pour le droit sur la protection des données. Si des allégements devaient néanmoins être prévus, il est proposé que, dans l'intérêt de l'unité de l'ordre juridique, ils s'appliquent non seulement aux prétentions fondées sur la LPD, mais également à celles fondées sur les art. 28 et la LCD ; il est précisé que seuls les consommateurs devraient pouvoir en bénéficier. *Plusieurs membres du groupe d'accompagnement* sont d'avis que les allégements ne devraient pas être réservés aux personnes physiques, mais que, le cas échéant, les entreprises devraient également pouvoir en profiter.

Prises de position de l'autorité de contrôle : étant donné la haute technicité de la matière, il peut arriver que l'appréciation juridique des litiges dans le domaine de la protection des données pose certaines difficultés. Dans la mesure où l'autorité de contrôle est un organe spécialisé en la matière, il devrait être possible de lui demander une prise de position dans des procédures de droit civil. Le groupe d'accompagnement propose ce qui suit : si une procédure civile porte sur la licéité d'un traitement de données, le tribunal peut, d'office ou à la demande d'une partie, soumettre l'affaire à l'autorité de contrôle pour prise de position. Celle-la n'est pas tenue de prendre position. Si elle le fait, le tribunal n'est pas obligé d'en tenir compte, et ne perd ainsi pas sa compétence décisionnelle (principe de l'indépendance du pouvoir judiciaire).

Exercice collectif des droits : la LPD ne contient pas de disposition particulière concernant l'exercice collectif des droits des personnes concernées. Ce sont donc les règles usuelles de la procédure civile qui s'appliquent en la matière.

Le Conseil fédéral a rendu un rapport sur l'exercice collectif des droits en Suisse en 2013[75]. Il y relève que le droit privé suisse connaît déjà certains instruments d'exercice collectif des droits, tels le cumul subjectif et objectif d'actions (art. 71 et 90 CPC), la jonction de cause, la suspension de la procédure et le renvoi (art. 125, let. c, 126 et 127 CPC) ou encore l'action des organisations (art. 89 CPC). Il considère que ces instruments ne sont pas toujours adéquats s'agissant de la réparation des dommages collectifs dispersés et propose plusieurs mesures pour améliorer la situation. Parmi celles-ci figurent l'extension du champ d'application de l'action des organisations à tous les domaines juridiques, voire aux actions en réparation, ou l'instauration de véritables instruments de mise en œuvre collective des droits. Dans cette seconde hypothèse, le Conseil fédéral parle soit de créer les bases légales pour des actions modèles (ou test)[76], soit d'introduire une action de groupe[77]. Deux

---

d'assurance sociale; b. des discriminations à raison du sexe; c. des litiges résultant de rapports de travail, pour autant que la valeur litigieuse ne dépasse pas 30 000 francs; d. des litiges concernant les art. 7 et 8 de la loi du 13 décembre 2002 sur l'égalité pour les handicapés. » (al. 4) « Si des motifs particuliers le justifient, le Tribunal fédéral peut majorer ces montants jusqu'au double dans les cas visés à l'al. 3 et jusqu'à 10 000 francs dans les cas visés à l'al. 4. » (al. 5).

[75] Rapport du Conseil fédéral du 3 juillet 2013 « Exercice collectif des droits en Suisse : état des lieux et perspectives ».

[76] L'action modèle ou action test permet de sauvegarder des intérêts collectifs en réalisant tout d'abord une seule « procédure modèle » typique entre deux parties sur une question litigieuse précise. La décision rendue entre ces deux parties aura alors valeur d'exemple procédural, concernant certaines questions de fait ou de droit, pour des litiges ultérieurs entre d'autres parties, de sorte que ces procédures ne devront plus répondre à la même question litigieuse. Il s'agit toujours d'une action individuelle du demandeur modèle, dont l'objectif est que le règlement des questions de fait ou de droit dans la procédure modèle ait un effet externe pour quantité de cas. La condition préalable de cet effet externe de la force de chose jugée est l'existence soit d'une base légale correspondante,

modèles seraient alors envisageables :

- l'introduction d'une action de groupe avec un système d'opt-in (le droit suisse connaît déjà des instruments juridiques qui se rapprochent très fortement de l'action de groupe)[78];
- l'introduction d'une procédure spéciale de transaction de groupe, inspirée des règles néerlandaises (extension par le juge de la force obligatoire d'une transaction à tous les lésés).

À noter qu'il n'a jamais été question d'instaurer une « class action » à l'américaine en raison notamment des risques d'abus qu'elle implique, engendrés partiellement par les conditions-cadres matérielles et procédurales en vigueur aux États-Unis[79].

Suite au rapport précité, la conseillère nationale Birrer-Heimo a déposé une motion[80] demandant au Conseil fédéral de modifier la loi afin qu'un grand nombre de personnes lésées de manière identique ou similaire puissent faire valoir collectivement leurs prétentions devant le juge. Le Conseil fédéral a répondu qu'il estimait inopportun d'élaborer une loi sur l'exercice collectif des droits (loi sur les actions collectives), mais s'est déclaré prêt à proposer des modifications ponctuelles allant dans le sens de son rapport sur l'exercice collectif des droits ou à prendre les aspects qui y sont exposés en compte dans les travaux législatifs en cours, par exemple dans la révision du droit de la société anonyme et dans la loi sur les services financiers en cours d'élaboration. La motion a été adoptée le 12 juin 2014.

La question se pose de savoir s'il faut introduire dans la LPD des instruments d'exercice collectif des droits, comme cela est d'ailleurs demandé par la motion Schwaab 13.3052 « Droit d'action collective en cas de viol de la protection des données, en particulier sur Internet »[81].

---

ou, en l'absence de base légale (comme en Suisse), d'une convention correspondante entre les parties (Rapport du Conseil fédéral du 3 juillet 2013, pp. 28 s.).

[77] Les actions de groupe sont des actions représentatives, où les prétentions individuelles sont regroupées de par le fait qu'un demandeur du groupe agit en faveur d'autres personnes. Ces dernières ne sont pas formellement parties à la procédure, mais participent tout de même au résultat, car la force de chose jugée s'étend également à leurs prétentions. La forme la plus connue d'action de groupe est l'action collective sur le modèle américain (« class action »). Selon la manière dont les tiers participent au résultat de la procédure aux côtés du demandeur de groupe, on distingue les actions de groupe avec option d'adhésion (opt-in) et les actions de groupe avec option de retrait (opt-out). Les deux modèles prévoient une procédure d'information des membres du groupe, celle-ci ayant toutefois une portée très différente dans les deux modèles. Outre les personnes individuelles touchées, des associations (à but idéal) ou des autorités sont également susceptibles de tenir le rôle de demandeurs de groupe. Les demandeurs de groupe sont en principe soumis à des exigences particulières, car ils agissent, au-delà de leurs propres intérêts, en tant que représentants du groupe et que leurs actes ont des effets pour tous les membres du groupe (Rapport du Conseil fédéral du 3 juillet 2013, pp. 32 s.).

[78] Action en examen des parts sociales et du sociétariat selon l'art. 105 de la loi sur la fusion (LFus; RS 221.301); représentant de la communauté des investisseurs selon l'art. 86 de la loi sur les placements collectifs (LPCC, RS 951.31); ou encore, dispositions spéciales pour le traitement des prétentions en responsabilité pour des dommages d'origine nucléaire (cf. art. 20 ss de loi fédérale du 13 juin 2008 sur la responsabilité civile en matière nucléaire [nLRCN; FF 2008 4843, 4845; pas encore entrée en vigueur]), voir Rapport du Conseil fédéral du 3 juillet 2013, pp. 33 ss.

[79] Sur ces questions, voir Rapport du Conseil fédéral du 3 juillet 2013, pp. 32 s.

[80] Motion Birrer-Heimo du 27 septembre 2013 13.3931 « Exercice collectif des droits. Promotion et développement des instruments ».

[81] La motion Schwaab 13.3052 du 7 mars 2013 n'a pas encore été traitée au Conseil national.

Une majorité du groupe d'accompagnement estime qu'il convient de renoncer à l'introduction de mesures particulières dans la LPD, pour deux raisons principalement. Premièrement, l'art. 89 CPC permet déjà à certaines organisations d'intenter des actions défensives en cas d'atteinte à la personnalité de membres de groupes déterminés et de solliciter du juge l'interdiction et la cessation de l'atteinte, la constatation de son caractère illicite, la publication de la rectification ou du jugement ainsi qu'un droit de réponse. Deuxièmement, en droit de la protection des données, les cas de dommages de masse ou dispersés sont plutôt rares, qu'ils soient financiers ou résultent d'un tort moral, et il paraît peu opportun d'introduire dans la LPD des mesures particulières en ce sens. Le renforcement des compétences et des pouvoirs de l'autorité de contrôle paraît plus à même d'assurer la mise en œuvre de la loi (cf. ch. 4.10.2).

Une minorité du groupe d'accompagnement est en revanche d'avis que les instruments d'exercice collectif des droits devraient être renforcés. Elle propose d'examiner la possibilité d'étendre l'art. 89 CPC aux cas dans lesquels seul un, ou peu des membres d'un groupe subissent une atteinte à la personnalité (en particulier lorsque le litige est susceptible de se reproduire et/ou est susceptible de concerner un grand nombre de personnes). Les individus pourraient ainsi être soulagés des risques du procès et confier la chose à une organisation disposant des moyens techniques et juridiques nécessaires. Il est aussi souhaité que l'art. 89 CPC soit étendu aux actions en réparation. Cumulativement à ces extensions, cette partie du groupe d'accompagnement souhaite que l'on introduise une action de groupe, avec un système d'opt-in, ou une procédure spéciale de transaction de groupe inspirée du modèle néerlandais, tant pour les actions défensives que pour les actions en réparation.

c) Mécanismes alternatifs de règlement des litiges

Outre les mesures décrites ci-dessus, le groupe d'accompagnement a également étudié l'opportunité d'introduire des mécanismes alternatifs de règlement des litiges en matière de protection des données (en particulier médiation, ombudsman)[82]. De telles procédures pourraient contribuer à régler des conflits le plus tôt possible et à l'amiable et permettraient ainsi aux parties d'épargner des frais et d'autres investissements. Les personnes désireuses de trouver une solution pragmatique à leur différend pourraient préserver leurs droits sans devoir entamer de procédure formelle. Une procédure de médiation permettrait également de prendre en compte les besoins particuliers des mineurs et de décharger considérablement les autorités (autorité de contrôle, tribunaux civils et juridictions administratives).

Au moment de l'entrée en vigueur de la LPD, l'intention du législateur était de conférer au PFPDT le rôle d'ombudsman ou de médiateur en cas de différends entre des privés et des organes fédéraux traitant des données [83]. Vu les compétences de rendre des décisions et de prononcer des sanctions dont sera éventuellement investie l'autorité de contrôle (cf. plus bas, ch. 4.10.2), certains membres du groupe d'accompagnement ont émis des réserves, estimant que le cumul d'une activité de médiation et d'un pouvoir décisionnel auprès d'une même autorité pourrait entraîner des conflits. Il est toutefois pensable que l'autorité de contrôle intervienne autant que possible dans le sens d'une médiation dans le cadre de ses tâches, sans qu'il s'agisse d'une médiation classique.

---

[82] Voir aussi l'art. 10 du projet de modernisation de la Convention STE 108 : « Chaque Partie s'engage à établir des sanctions et recours juridictionnels et non-juridictionnels appropriés visant les violations du droit interne donnant effet aux dispositions de la présente Convention. »

[83] Cf. le message du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421, 487.

Le groupe d'accompagnement propose ce qui suit pour ce qui est de la mise en place d'une procédure alternative de résolution des litiges: les différentes branches économiques doivent avoir la possibilité de créer ou de désigner, dans le cadre de l'autoréglementation (cf. ch. 4.1.2, let. b), un service chargé des procédures de conciliation ou de médiation relatives à des litiges en matière de protection des données. Si ces tâches étaient confiées à des bureaux d'ombudsman déjà existants, ceux-ci devraient former leur personnel dans le domaine de la protection des données. En l'absence d'une solution de branche, l'autorité de contrôle pourrait désigner un service de médiation ou un bureau d'ombudsman, à l'instar de ce que prévoit la législation sur la radio et la télévision.[84] La procédure de conciliation serait facultative.

Le groupe d'accompagnement a par ailleurs examiné la possibilité de désigner comme ombudsman les autorités de contrôle cantonales, mais l'a rejetée. Plusieurs membres du groupe sont d'avis qu'une telle attribution aboutirait à un mélange des compétences fédérales et cantonales. Ils doutent d'ailleurs que les cantons approuvent une modification de l'actuelle répartition des compétences. Qui plus est, les cantons rencontrent également des problèmes de ressources dans le domaine de la surveillance de la protection des données.

4.9 Dispositions particulières relatives au traitement de données personnelles par des organes fédéraux

4.9.1 Conception de la réglementation

Le droit sur la protection des données applicable au traitement de données personnelles par des organes de la Confédération se compose, outre de la législation générale en la matière (LPD et OLPD), de nombreuses dispositions prévues dans des lois spéciales. Le groupe d'accompagnement a examiné la question de savoir s'il ne faudrait pas rassembler dans un seul acte normatif l'ensemble des dispositions contenues dans ces lois spéciales, afin de disposer d'une seule loi régissant les traitements des données dans les différents domaines étatiques fédéraux. Il a conclu qu'une telle mesure n'était pas nécessaire du point de vue légistique et a par conséquent décidé de maintenir le système actuel. Des dispositions sur la protection des données spécifiques aux différents domaines permettent d'ailleurs de mieux tenir compte des objectifs poursuivis par les lois spéciales (cf. plus haut, ch. 4.1.1).

Le groupe d'accompagnement n'a pas non plus identifié de besoin d'agir s'agissant du champ d'application matériel des dispositions de droit public sur la protection des données, ou desexceptions régissant les activités de droit privé exercées par des organes fédéraux (art. 23 LPD).

4.9.2 Licéité du traitement de données (en particulier bases légales suffisantes)

Il est prévu de conserver les exigences posées à l'art. 17 LPD concernant les bases légales d'un traitement de données ainsi que le principe de l'autorisation spéciale, qui veut que la base légale exigée ne soit pas déjà donnée par la LPD, mais figure dans une réglementation spécifique dans le domaine concerné. Le groupe d'accompagnement estime toutefois que la conception de l'art. 17, al. 2, LPD, qui règle les cas dans lesquels une base légale n'est pas exigée (Surrogat für Rechtsgrundlage), manque de clarté. Il propose dès lors de revoir cette disposition, en particulier de préciser que l'exception mentionnée à l'art. 17, al. 2, let. c, LPD se rapporte non seulement au traitement de données personnelles sensibles, mais égale-

[84] Voir les art. 18 ss du règlement de l'autorité indépendante d'examen des plaintes en matière de radio télévision (RS 784.409).

ment à celui de données personnelles « ordinaires » selon l'art. 17, al. 1, LPD.

Il n'apparaît pas nécessaire au groupe d'accompagnement de fixer d'autres exigences dans la LPD concernant la formulation de bases légales relatives au traitement de données dans des domaines spécifiques. Il renvoie à cet égard à l'accompagnement législatif fait par l'Office fédéral de la justice, dans le cadre duquel l'existence et la suffisance des bases légales spéciales sont examinées et au fait que l'autorité de contrôle est invitée à se prononcer sur les projets d'actes législatifs (cf. art. 31, al. 1, let. b, LPD). Ces différents instruments garantissent que les exigences générales en matière de protection des données sont également respectées dans les réglementations sectorielles.

Une *partie du groupe d'accompagnement* propose toutefois d'examiner s'il ne serait pas judicieux de fixer dans la LPD les exigences essentielles concernant les bases légales pour les systèmes d'information. Selon la pratique actuelle[85] en effet, de très nombreux détails doivent être arrêtés au niveau de la loi formelle.

La disposition relative au traitement de données automatisé dans le cadre d'essais pilotes n'a joué qu'un rôle mineur dans la pratique (art. 17a LPD). Le groupe d'accompagnement estime par conséquent judicieux de faciliter cette procédure. Il propose d'attribuer la compétence d'évaluer l'autorisation (par décision) à l'autorité de contrôle, en lieu et place du Conseil fédéral. Cette disposition devrait par ailleurs être raccourcie et les détails réglés au niveau ordonnance. L'art. 17a LPD porte sur une exception à l'exigence d'une base légale pour traiter des données personnelles sensibles. Pour des raisons de systématique, cette exception ne devrait pas être réglée séparément, mais devrait figurer à l'art. 17, al. 2, LPD.

4.9.3 Dispositions particulières pour certaines formes de traitement de données

La LPD contient des prescriptions particulières à l'intention des organes fédéraux pour différentes formes de traitement (p. ex. collecte, communication, anonymisation ou destruction). Ces dispositions ont dans l'ensemble fait leurs preuves.

Dispositions particulières relatives à la communication de données personnelles : le rapport entre l'art. 19 LPD (communication de données personnelles) et l'art. 17 LPD (bases juridiques), spécialement en ce qui concerne les exceptions à l'exigence de la base légale pour communiquer des données personnelles sensibles, doit être clarifié. Selon le groupe d'accompagnement l'art. 19 LPD doit se rapporter à toutes les données personnelles, y compris au données sensibles. Il propose également d'étendre le catalogue des exceptions de l'art. 19 LPD, en ce sens que la communication de données personnelles par des organes fédéraux est autorisée même en l'absence de base légale, lorsque cela est nécessaire pour protéger des intérêts prépondérants ou vitaux (p. ex. la vie ou l'intégrité physique) de la personne concernée ou de tiers. Enfin, le groupe d'accompagnement est d'avis que l'art. 19, al. 3, LPD qui concerne la mise à disposition en ligne des données (procédure d'appel) peut être abrogé. Avec l'évolution de la technique, l'accès en ligne est devenu courant ; il n'est donc plus aussi imprévisible pour les personnes concernées qu'il ne l'était au moment de l'introduction de cette disposition. Le groupe d'accompagnement estime que l'exigence de la base légale énoncée à l'art. 19, al. 1, LPD est suffisante à cet égard.

Dispositions particulières relatives au devoir d'informer lors de la collecte de données *:* voir le ch. 4.3.1. Il faut relever à ce propos que la teneur de l'art. 18 LPD est d'ores et déjà couverte par celle de l'art. 18a LPD. L'art. 18 LPD peut donc être abrogé.

---

[85] Voir à ce propos le Guide de l'OFJ du 16 décembre 2010 pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles.

4.9.4 Mesures organisationnelles

Il convient de renforcer et d'encourager la responsabilisation des organes fédéraux en ce qui concerne le respect des dispositions sur la protection des données. À cet effet, il faudrait que les conseillers à selon l'art. 23 OLPD que doivent désigner la Chancellerie fédérale et chaque département, aient les mêmes tâches et la même position que les « conseillers» selon les art. 12a et 12b OLPD (voir plus haut, ch. 4.3.2)[86]. Cela signifie en particulier que les premiers cités doivent pouvoir exercer leur activité de façon indépendante sur le plan organisationnel et professionnel, et disposer des ressources nécessaires à cet effet. Un renforcement de la position des conseillers internes de l'administration pourrait par ailleurs contribuer à décharger l'autorité de contrôle.

4.9.5 Prétentions et procédures

a) Prétentions

Comme cela a été expliqué aux ch. 4.4.1 et 4.4.2, les différentes prétentions en matière de protection des données doivent être réunies dans un catalogue commun pour les secteurs public et privé. Cette simplification doit améliorer la lisibilité de la LPD et donner aux personnes concernées une meilleure vue d'ensemble de leurs droits à l'encontre des auteurs de traitements de données. En revanche, il ne faut rien changer matériellement à l'actuel système d'excercie des droits (p. ex. s'agissant de la légitimation active et passive ou des voies de recours). S'agissant du traitement de données par des organes fédéraux, il convient toutefois d'examiner de plus près s'il ne faudrait pas, par analogie à la solution retenue en droit privé, introduire un droit d'opposition pour tous les traitements. Actuellement, les personnes concernées peuvent uniquement exiger de l'organe fédéral responsable qu'il ne communique pas des données personnelles déterminées à des tiers (art. 20 LPD).

Les actions en dommages-intérêts ou en réparation pour tort moral doivent continuer à obéir aux conditions générales du droit de responsabilité de l'Etat. Les conséquences financières de traitements de données illicites continueront donc à être appréciées sous l'angle des art. 3 ss de la loi sur la responsabilité (LRCF ; RS 170.32).

b) Répartition du fardeau de la preuve

Les personnes concernées doivent bénéficier d'un allégement du fardeau de la preuve lorsqu'elles font valoir leurs droits à l'encontre d'organes fédéraux, comme le propose le groupe d'accompagnement pour les traitements de données par des privés (cf. ch. 4.8.2). Il s'agit en l'occurrence d'un renversement du fardeau de la preuve, sur le modèle de l'art. 13a, al. 1, LCD[87], à savoir qu'il peut être exigé de l'organe fédéral, de prouver qu'il se conforme au droit de la protection des données si, compte tenu des intérêts légitimes des parties à la procédure, une telle exigence paraît appropriée (concernant la présomption légale de la régularité d'un traitement de données lorsque les règles de bonnes pratiques sont respectées, voir plus haut, ch. 4.1.2, let. b). Tel pourrait être le cas lorsque l'administration des preuves est particulièrement difficile pour la personne concernée, par exemple quant les faits sont dans la sphère d'influence de l'auteur du traitement (p. ex. en rapport avec le respect du devoir de

---

[86] Concernant les tâches et la position des conseillers à la protection des données (Datenschutzverantwortliche), voir les explications sur le site du PFPDT, http://www.edoeb.admin.ch/datenschutz/00626/00743/00874/01051/index.html?lang=fr.

[87] Art. 13a, al. 1, LCD: « Le juge peut exiger que l'annonceur apporte des preuves concernant l'exactitude matérielle des données de fait contenues dans la publicité si, compte tenu des intérêts légitimes de l'annonceur et de toute autre partie à la procédure, une telle exigence paraît appropriée en l'espèce. »

diligence selon le ch. 4.3.2).

c) Dispositions de procédure

L'évaluation de la loi sur la protection des données a montré que les personnes concernées vont plus souvent en procédure contre des organes fédéraux que contre des privés. Dans l'absolu, les prétentions sont toutefois rarement exercées dans le secteur public également[88]. Il n'y a selon le groupe d'accompagnement que peu d'options pour améliorer la protection juridique individuelle dans la procédure de droit public (comme dans la procédure civile d'ailleurs). En clair, la mise en œuvre des dispositions de droit public sur la protection des données doit prioritairement passer par une extension des compétences de l'autorité de contrôle (cf. ch. 4.10.2).

Comme pour la procédure civile, le groupe d'accompagnement propose de prévoir pour les autorités administratives de première instance ou de recours la possibilité de demander une prise de position à l'autorité de contrôle (cf. ch. 4.8.3, let. b): si une procédure porte sur l'admissibilité d'un traitement de données, l'autorité administrative compétente ou l'instance de recours peut, d'office ou à la demande d'une partie, soumettre l'affaire à l'autorité de contrôle pour prise de position. Celle-ci n'est pas tenue de se prononcer. Si elle le fait, son avis n'est pas contraignant.

d) Modes alternatifs de règlement des litiges

Il est prévu de proposer, comme pour le secteur privé, un mode alternatif pour le règlement des litiges ayant trait au traitement de données par des organes fédéraux. La procédure seraitêtre confiée à un service de médiation ou d'ombudsman à désigner par l'autorité de contrôle (cf. ch. 4.8.3, let. c).

4.9.6 Relation entre les dispositions de la LPD et de la LTrans

La loi fédérale sur le principe de la transparence dans l'administration (LTrans ; RS 152.3) présente plusieurs points de recoupement avec la LPD. Or, la LTrans fait actuellement l'objet d'une évaluation concernant sa mise en œuvre et son efficacité. Il apparaît par conséquent au groupe d'accompagnement peu opportun de formuler en ce moment des propositions tombant dans le champ d'application de cette loi[89].

4.10 Autorités de contrôle

4.10.1 Introduction

On l'a vu, l'évaluation de la LPD a mis pour *une majorité du groupe d'accompagnement* en évidence des lacunes dans la mise en œuvre (« Durchsetzung ») de la loi. Ces carences peuvent certes être atténuées par un renforcement des droits procéduraux des parties et un accès à la justice facilité. Le groupe d'accompagnement estime cependant qu'on ne peut réellement améliorer l'efficacité de la loi sans renforcer de manière significative les pouvoirs de l'autorité de contrôle, en lui conférant un pouvoir de décision (voir les réflexions menées au ch. 4.1.2, let. a). Le projet de modernisation de la Convention STE 108 prévoit aussi une

---

[88] Schlussbericht zur Evaluation des Bundesgesetzes über den Datenschutz du 10 mars 2011, pp. 86 ss, 133 ss, 208; disponible en ligne (en allemand) <https://www.bj.admin.ch/dam/data/bj/staat/evaluation/schlussber-datenschutzeval-d.pdf>.

[89] Cf. l'évaluation de la LTrans <http://www.admin.ch/aktuell/00089/index.html?lang=fr&msg-id=52653>. L'OFJ soumettra au Conseil fédéral son rapport concernant les résultats de cette évaluation d'ici à la fin de 2014. Peut-être faudra-t-il intégrer ces conclusions dans la suite des travaux de révision de la LPD.

telle compétence. Dans cette entreprise, une attention toute particulière devrait être portée au maintien, voire à l'amélioration de l'indépendance de l'autorité de contrôle, qui est un thème toujours actuel, en Suisse[90], mais aussi au plan européen[91].

Compte tenu des compétences et pouvoirs plus étendus que le groupe d'accompagnement propose de conférer au PFPDT, la question de savoir s'il ne serait pas adéquat de modifier son organisation pour en faire une autorité collégiale se pose. Des propositions en ce sens sont faites au ch. 4.10.3 ci-dessous.

À noter *qu'une minorité du groupe d'accompagnement* s'oppose à ce que les pouvoirs de l'autorité de contrôle – en particuliers de décision et de sanction – soient renforcés. Des éventuelles modifications législatives ne devraient par ailleurs intervenir à ses yeux que dans la mesure de ce qui est nécessaire, en regard du droit UE et du projet de modernisation de la Convention STE 108, pour l'accès au marché (cf. ch. 3).

4.10.2 Tâches et pouvoirs de l'autorité de contrôle

a) Dans le secteur privé

aa) Surveillance des personnes privées

Réalisation d'une enquête préalable *:* le groupe d'accompagnement propose d'introduire une procédure d'enquête préalable sur le modèle de l'art. 26 LCart[92]. Cette procédure serait très informelle et le plus simple possible afin de faciliter la recherche de solutions à l'amiable. Il ne s'agirait pas d'une étape obligatoire et l'autorité pourrait, dans certains cas, ouvrir directement une procédure formelle.

La procédure préalable aurait comme fonction d'assurer le tri des affaires nécessitant l'ouverture d'une enquête proprement dite, et permettrait aux particuliers, notamment aux personnes dont les données font l'objet d'un traitement, de s'adresser facilement à l'autorité de contrôle pour lui demander des conseils. Elle serait menée par le secrétariat permanent de l'autorité de contrôle (cf. ch. 4.10.3). Cette dernière pourrait ouvrir une enquête préalable d'office, à la demande des personnes concernées par un traitement de données, ou sur dénonciation de tiers. Elle n'aurait pas l'obligation de le faire, et il n'existerait pas de voie de recours contre un refus d'entrer en matière. La procédure serait gratuite.

Au terme de l'enquête préalable, l'autorité de contrôle aurait plusieurs options. En l'absence d'indices sur la présence d'une situation justifiant l'ouverture d'une enquête formelle (art. 29 LPD), elle en informerait simplement par écrit les intervenants. En présence d'indices sur la présence d'une situation justifiant l'ouverture d'une enquête, elle pourrait :

– Proposer des mesures pour supprimer ou empêcher une violation de la LPD. L'approbation de la proposition par l'auteur du traitement ne constituerait pas un accord à l'amiable dont la violation pourrait être sanctionnée. Il s'agirait de simples engagements unilatéraux, qui ne seraient soumis à aucune forme. En cas de respect des engagements pris, l'autorité de contrôle n'ouvrirait pas d'enquête.

---

[90] Rapport du Conseil fédéral sur l'évaluation de la loi sur la protection des données du 9 décembre 2011, FF 2012 255 ss, 269.

[91] Arrêts de la CJUE C-614/10 du 16 octobre 2012 et C-288/12 du 8 avril 2014.

[92] Art. 26 LCart : « Le secrétariat peut mener des enquêtes préalables d'office, à la demande des entreprises concernées ou sur dénonciation de tiers. » (al. 1). « Il peut proposer des mesures pour supprimer ou empêcher des restrictions à la concurrence. » (al. 2). « La procédure d'enquête préalable n'implique pas le droit de consulter les dossiers. » (al. 3).

– Ouvrir une enquête formelle.

L'information et les propositions de l'autorité de contrôle, de même que l'ouverture de l'enquête, ne seraient pas sujettes à recours.

Ouverture d'une enquête formelle : le groupe d'accompagnement propose de ne plus limiter le champ du pouvoir d'enquête de l'autorité de contrôle aux cas prévus à l'actuel art. 29 LPD. En raison de ses ressources limitées, l'autorité de contrôle devra toutefois dans les faits se concentrer sur les cas qui présentent un intérêt public et définir ses priorités.

Instruction lors de la procédure d'enquête formelle : afin que l'autorité de contrôle puisse établir les faits le plus rapidement et le plus exactement possible, le groupe d'accompagnement propose de renforcer ses pouvoirs d'instruction. Outre la possibilité de demander aux responsables de traitements qu'ils lui fournissent tous les renseignements et documents nécessaires et lui présentent les traitements (art. 29 al. 2 LPD), elle pourrait à certaines conditions également demander à pouvoir accéder aux locaux et aux programmes informatiques, effectuer des saisies ou faire poser des scellés. La procédure serait régie par la loi fédérale sur la procédure administrative (PA ; RS 172.021), voire, par analogie et selon les mesures envisagées, par la loi fédérale sur le droit pénal administratif (LPA ; RS 313.0; art. 45 ss).

Pouvoirs de décision et de sanction [93]: l'autorité de contrôle aurait un pouvoir de décision, c'est-à-dire qu'elle pourrait imposer des mesures, telles la suspension ou la cessation d'un traitement de données. Elle aurait également le pouvoir de prononcer, à certaines conditions, des sanctions pécuniaires. Concrètement, si l'autorité de contrôle, au terme de son enquête formelle, constate que le traitement n'est pas conforme à la loi, elle impartirait un délai au responsable pour régulariser la situation. Elle pourrait parallèlement proposer un accord à l'amiable, de manière analogue à ce que prévoit l'art. 29 LCart[94] par exemple. Si la situation n'est pas régularisée au terme du délai fixé, ou en exécution de l'accord à l'amiable, l'autorité de contrôle pourrait rendre une décision interdisant ou suspendant le traitement et/ou enjoignant au responsable du traitement de prendre des mesures. En cas de non-respect d'une décision entrée en force ou de non-respect d'un accord à l'amiable, l'autorité de contrôle pourra prononcer une sanction pécuniaire. Dans certains cas de violation crasse de la loi, l'autorité pourrait directement (c'est-à-dire sans passer par l'accord à l'amiable ou la fixation d'un délai) prononcer une sanction pécuniaire, et ce cumulativement à une mesure (interdiction, suspension, autres mesures). Au surplus, le refus de collaborer pourrait aussi être sanctionné. Dans tous les cas, l'autorité de contrôle pourrait prendre les mesures provisionnelles nécessaires.

➢ Variante : une partie du groupe de travail propose que l'autorité de contrôle ne sanctionne pas elle-même le non-respect de ses décisions entrées en force, mais qu'elle mentionne dans les dispositifs de ces dernières l'art. 292 du code pénal suisse (CP ; RS 311.0). La poursuite incomberait alors aux cantons.

Le groupe d'accompagnement s'est demandé s'il fallait conférer à la personne qui a signalé le cas à l'autorité de contrôle la qualité de partie à la procédure et ou la qualité pour recourir.

---

[93] La Commission des institutions politiques du Conseil national (CIP-CN) a décidé, le 29 août 2014, de ne pas donner suite à l'initiative parlementaire Schwaab 14.404 du 19 mars 2014 « Pour des sanctions réellement dissuasives en cas de violation de la protection des données ».

[94] Art. 29 LCart: « Si le secrétariat considère qu'une restriction à la concurrence est illicite, il peut proposer aux entreprises concernées un accord amiable portant sur les modalités de la suppression de la restriction. »(al. 1). « L'accord requiert la forme écrite et doit être approuvé par la commission. » (al. 2).

Il propose d'y renoncer, dans la mesure où l'autorité de contrôle doit à l'avenir rester une garante de l'intérêt public, et non trancher des litiges individuels.

Pour faciliter la mise en œuvre de la loi en présence d'auteurs de traitements qui n'ont pas de siège (domicile) en Suisse, il est prévu de les obliger à fournir, dans le cadre des investigations menées par l'autorité de contrôle, une adresse de correspondance en Suisse à laquelle des décisions pourraient leur être valablement notifiées.[95] Le non-respect de cette obligation serait sanctionné.

ab) Conseil aux privés

L'activité de conseil aux personnes privées, telle que prévue par l'actuel art. 28 LPD, est maintenue.

Pour ce qui est du conseil aux responsables de traitement, le groupe d'accompagnement propose d'introduire une sorte de procédure d'examen préalable semblable à ce qui existe en droit des cartels afin d'éviter notamment que la double activité de conseil et de contrôle de l'autorité de contrôle ne les dissuade de s'adresser à elle. À la différence de la notification prévue dans la LCart, l'annonce serait facultative. Il s'agirait de permettre au responsable du traitement de connaître les éventuelles objections de l'autorité de contrôle avant la mise en œuvre d'un nouveau traitement et d'éviter par la suite des sanctions pécuniaires. Pratiquement, la personne pourrait soumettre les traitements de données envisagés à l'autorité, qui aurait alors un certain délai (p. ex. un mois) pour décider s'il y a lieu de procéder à un examen du traitement (sur le modèle de l'art. 32 LCart[96]). Faute de communication de la part de l'autorité de contrôle dans ce délai, le traitement pourrait être effectué sans encourir le risque d'une sanction de l'autorité, pour autant que le traitement effectué soit celui annoncé. Il y aurait lieu de prévoir, de manière analogue à l'art. 38 LCart[97], des conditions qui permettraient, malgré l'écoulement du délai, de procéder à un examen (p. ex. le responsable du traitement a fourni des données inexactes, il existe un risque d'atteinte grave qui ne pouvait être détecté sur la base des informations fournies, etc.). S'il existe des règles de bonnes pratiques en la matière (cf. ch. 4.1.2 let. b), et que l'auteur du traitement s'y conforme, il n'encourrait aucune sanction pécuniaire. S'il soumet son cas à l'autorité malgré l'existence de règles de bonnes pratiques, cette dernière pourrait se contenter d'y renvoyer sans examen au fond. En l'absence de règles de bonnes pratiques, l'autorité pourrait suggérer au comité

---

[95] On trouve par exemple une prescription de ce type à l'art. 5 de l'ordonnance sur les services de télécommunication (OST, RS 784.101.1): « Les fournisseurs de services de télécommunication obligés de s'annoncer dont le siège se trouve à l'étranger doivent indiquer une adresse de correspondance en Suisse à laquelle des communications, des citations et des décisions peuvent notamment leur être valablement notifiées. »

[96] Art. 32 LCart: « A la réception de la notification d'une concentration d'entreprises (…), la commission décide s'il y a lieu de procéder à un examen de l'opération de concentration. La commission communique, dans le délai d'un mois à compter de la notification de l'opération de concentration, l'ouverture de l'examen de la concentration aux entreprises participantes. Faute de communication dans ce délai, la concentration peut être réalisée sans réserve. » (al. 1). « Les entreprises participantes s'abstiennent de réaliser la concentration pendant le délai d'un mois suivant sa notification, à moins que, à leur requête, la commission ne les ait autorisées à le faire pour des motifs importants. » (al. 2).

[97] Art. 38 LCart: 1 « La commission peut rapporter une autorisation ou décider l'examen d'une concentration malgré l'écoulement du délai de l'art. 32, al. 1, lorsque: a. les entreprises participantes ont fourni des indications inexactes; b. l'autorisation a été obtenue frauduleusement; c. les entreprises participantes contreviennent gravement à une charge dont a été assortie l'autorisation. » (al. 1). « Le Conseil fédéral peut rapporter une autorisation exceptionnelle pour les mêmes motifs. » (al. 2).

compétent d'édicter de telles règles pour le cas en question.

b) Dans le secteur public

ba) Surveillance des organes fédéraux

Le groupe d'accompagnement propose de renforcer la surveillance des organes fédéraux également, dans la mesure du possible de manière analogue à ce que qui est prévu pour le secteur privé (cf. ch. 4.1.1).

Réalisation d'une enquête préalable : le groupe d'accompagnement propose d'introduire une enquête préalable comme dans le secteur privé (cf. 4.10.2, let. a/aa).

Ouverture d'une enquête formelle : lorsque l'enquête préalable aura démontré des indices de violation des prescriptions sur la protection des données, ou en cas de violation claire, l'autorité pourrait ouvrir une enquête formelle (cf. ch. 4.10.2, let. a/aa).

Instruction lors de la procédure d'enquête : outre les pouvoir dont elle dispose déjà, le groupe d'accompagnement propose que l'autorité de contrôle soit autorisée à consulter par procédure d'appel les données traitées par les organes fédéraux. L'accès durerait le temps de la procédure.

Compétences de décision : le groupe d'accompagnement propose un modèle tel que le connaissent certains cantons (p. ex. Schauffhouse et Bâle-Ville). Il s'agirait de conférer à l'autorité de contrôle un pouvoir de décision, en plus de l'instrument de la recommandation prévu à l'actuel art. 27 LPD. L'idée est de renforcer les outils de contrôle et les compétences de l'autorité à l'encontre des organes fédéraux et d'améliorer la protection des données en prévision de la ratification de la Convention STE 108 modernisée et de la reprise du développement de l'acquis de Schengen/Dublin. Cette proposition permettrait par ailleurs d'harmoniser dans une certaine mesure les dispositions sur la protection des données dans les domaines public et privé. Concrètement, si l'autorité de contrôle constate une violation des prescriptions sur la protection des données, elle émet une recommandation à l'intention de l'organe fédéral responsable et en informe le département compétent ou la Chancellerie fédérale. Si la recommandation est rejetée ou n'est pas suivie, l'autorité peut transformer sa recommandation, en tout ou en partie, en une décision sujette à recours[98]. L'organe fédéral concerné peut attaquer cette décision selon les dispositions générales de l'organisation judiciaire fédérale. Il conviendrait en outre d'examiner l'opportunité d'investir l'autorité de contrôle de la compétence d'ordonner directement la restriction ou la cessation d'un traitement de données à titre de mesure provisoire[99]. Il faut encore déterminer dans quelle mesure ce modèle est susceptible d'entrer en collision avec la protection juridique conférée par l'art. 25 LPD. Qui plus est, il faut vérifier si une telle solution peut être intégrée dans le droit procédural public existant (PA, LTAF, LTF) et, le cas échéant, comment.

Une majorité du groupe d'accompagnement estime qu'il faut renoncer à ordonner des sanctions administratives (p. ex. des amendes) l'encontre des organe fédéraux, une pratique que

---

[98] Le canton de Bâle-Ville pose comme condition qu'il existe un intérêt prépondérant à mettre en œuvre la mesure recommandée. Pour plus de détails, voir le § 47, al. 1, 2 et 5, de la loi Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG BS; SG 153.260) ainsi que le § 26 s. de la loi Datenschutzgesetz des Kantons Schaffhausen (SHR 174.100).

[99] Cf. § 47, al. 4, IDG BS: « Si des intérêts dignes de protection sont visiblement menacés ou violés, le Préposé à la protection des données peut ordonner que l'organe public restreigne ou stoppe le traitement jusqu'à ce que la cour d'appel ait terminé son examen. » (traduction non officielle)

en vigueur dans plusieurs pays de l'UE (cf. ch. 4.1.2, let. a), du moins tant que l'acquis de Schengen/Dublin ne l'exige pas.

Les tiers qui auraient dénoncé le cas n'auraient ni la qualité de partie, ni la qualité pour recourir (cf. ch. 4.10.2, let. a/aa).

bb) Conseil aux organes fédéraux (art. 31, al. 2, LPD)

Cette activité de conseil doit être maintenue. Il s'agira d'adapter la rédaction de l'article dans le cas où l'exception de l'art. 2, al. 2, let. d, LPD devait être supprimée (voir ch. 4.10.2 let. d/db).

c) Elaboration de règles plus détaillées

La création de règles de bonnes pratiques ou de règles contraignantes, permettrait, on l'a vu (cf. ch. 4.1.2, let. b), de renforcer la sécurité du droit, dans la mesure où la LPD resterait très générale et technologiquement neutre.

La majorité du groupe d'accompagnement propose de confier l'élaboration de ces règles à un comité distinct de l'autorité de contrôle au sens étroit. Les règles de bonnes pratiques pourraient aussi être élaborées, d'office ou sur mandat des milieux concernés, qui les soumettraient à l'organe spécialisé, voire à l'autorité de contrôle pour approbation (cf. ch. 4.1.2, let. b).

d) Information et sensibilisation du public

La faculté pour l'organe de contrôle d'informer le public de ses constatations lorsqu'il en va de l'intérêt général est maintenue. Il s'agit d'un instrument de prévention important. Les éventuels secrets d'affaires ne doivent toutefois pas être mis en danger.

Le PFPDT sensibilise déjà actuellement la population, notamment par le biais d'informations sur son site internet. Le rapport d'évaluation a toutefois démontré que malgré cela, les personnes concernées ne prenaient pas toujours les précautions requises, soit parce qu'elles se sentent dépassées, soit encore parce qu'elles sous-estiment les possibilités d'exploitation de leurs données et les risques qui en découlent[100]. Le groupe d'accompagnement propose d'inscrire dans la loi, comme le fait le projet de modernisation de la Convention STE 108 (art. 12bis, al. 2, let. e) que l'autorité de contrôle est chargée de sensibiliser et d'éduquer la population à la protection des données. Cette sensibilisation pourra se faire par des règles de bonnes pratiques ou des règles contraignantes (cf. ch. 4.1.2, let. b), des campagnes d'information, voire encore des aides à la formation. Un effort particulier devra être fourni en rapport avec la question du consentement des personnes concernées (cf. ch. 4.3.3). Au surplus, il s'agira de porter une attention particulière aux mineurs et aux autres personnes vulnérables.

e) Prise de position dans une procédure civile ou administrative

Outre les tâches que l'autorité de contrôle exécute déjà, le groupe d'accompagnement propose, sur le modèle de l'art. 15 LCart[101], qu'en cas de procédure civile ou administrative, l'affaire puisse lui être transmise pour avis, à la demande d'une partie ou sur l'initiative du juge. Cela permettra d'éviter que des institutions non spécialisées aient à se prononcer seules, surtout en première instance, sur des cas parfois sensibles et techniques (cf.

---

[100] Cf. le rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi sur la protection des données, FF 2012 255ss, 261.

[101] Art. 15, al. 1, LCart: « Lorsque la licéité d'une restriction à la concurrence est mise en cause au cours d'une procédure civile, l'affaire est transmise pour avis à la Commission de la concurrence. »

ch. 4.8.3 let. b, et 4.9.5, let. c).

f) Procédure extrajudiciaire de résolution des litiges

Cf. ch. 4.8.3 let. c.

g) Fonction d'autorité de première instance

Une minorité du groupe d'accompagnement propose que l'autorité de contrôle ait une compétence générale de trancher les litiges en première instance en lieu et place du juge civil et des autorités administratives. Les actions en réparation demeureraient toutefois de la compétence de ces derniers. Cette solution aurait le mérite de faire trancher les litiges par une autorité spécialisée qui connaît bien le domaine. *Une majorité du groupe d'accompagnement* estime qu'il n'est pas judicieux de déroger au système ordinaire en instaurant une autorité spécialisée. Une telle solution constituerait une rupture dans notre ordre juridique et poserait un certain nombre de questions délicates qu'il conviendrait d'approfondir (mélange des rôles, problèmes de procédure, etc.). La possibilité évoquée plus haut de solliciter un avis de l'autorité de contrôle (cf. ch. 4.8.3, let. b, et 4.9.5, let. c) permettrait par ailleurs de suppléer d'une autre manière au manque de connaissances techniques des autorités ordinaires.

4.10.3 Organisation de l'autorité de contrôle

Le groupe d'accompagnement est divisé sur le modèle d'organisation à choisir pour l'autorité de contrôle. Certains estiment que, vu les nouveaux pouvoirs qu'il est prévu de lui conférer (cf. ch. 4.10.2), la forme de l'autorité collégiale serait plus indiquée. D'autres sont d'avis que le système actuel a fait ses preuves et qu'il n'y a pas de raison d'en changer. Dans les deux cas de figure, il se pose la question de savoir quelle serait l'autorité compétente pour adopter/avaliser les règles de bonnes pratiques ou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.1.2, let. b). *La majorité du groupe d'accompagnement* estime qu'il convient de confier cette tâche à un comité spécialisé, alors *qu'une minorité* est d'avis que c'est à l'autorité de contrôle elle-même d'assumer ce travail.

Compte tenu des avis divergents au sein du groupe d'accompagnement, les quatre modèles d'organisation suivants sont proposés : a) mise en place d'une autorité collégiale avec comité ; b) mise en place d'une autorité collégiale sans comité; c) maintien d'une autorité personnalisée avec comité et d) maintien d'une autorité personnalisée sans comité.

a) Autorité collégiale avec comité

Selon *une partie du groupe d'accompagnement*, le modèle de l'autorité collégiale assure une meilleure acceptation politique des éventuelles décisions et sanctions rendues. Il garantit également une prise de décision plus représentative et plus équilibrée, et permet de véritablement consolider les décisions au sein d'un collège. Le modèle collégial renforcerait par ailleurs l'indépendance de l'autorité de contrôle, dans la mesure où les éventuelles influences extérieures seraient en quelque sorte diluées par leur répartition entre les membres.

Au plan fédéral, la coutume est d'ailleurs plutôt de confier les tâches de surveillance à des autorités collégiales, telles la Commission de la concurrence (ComCo), la Commission fédérale des maisons de jeu (CFMJ), la Commission fédérale de l'électricité (ElCom), l'Institut suisse des produits thérapeutiques (Swissmedic), l'Autorité fédérale de surveillance des marchés financiers (FINMA) ou encore l'Institut Fédéral de la Propriété Intellectuelle (IPI)[102]. Le seul autre exemple d'autorité fédérale unipersonnelle est le Surveillant des prix. Sa situa-

[102] Voir le rapport du Conseil fédéral du 13 septembre 2006 sur l'externalisation et la gestion des tâches de la Confédération (rapport sur le gouvernement d'entreprise), FF 2006 7799 ss, en particulier pp. 7851 s.

tion n'est toutefois pas comparable à celle du PFPDT dans la mesure où il n'est pas indépendant, mais relève du Département fédéral de l'économie, de la formation et de la recherche (DEFR). Au plan cantonal, Neuchâtel/Jura, le Tessin, Fribourg et le Valais connaissent – avec des arrangements parfois différents – le modèle de la commission. Au plan international, on connaît également dans plusieurs pays soit le modèle de la commission (par ex. la « Commission Nationale de l'Informatique et des Libertés » [CNIL] en France), soit le modèle du directoire (le « Garante per la protezione dei dati personali » en Italie [composé de quatre membres] ou l'autorité néerlandaise « College bescherming persoonsgegevens » [CBP ; composée de trois membres]).

Le groupe d'accompagnement a examiné trois formes d'autorités collégiales : l'établissement, la commission et le directoire. Il a décidé d'écarter les deux premières, trop lourdes administrativement et susceptibles de ralentir les procédures. La forme de l'établissement ne paraissait au surplus pas opportune vu la taille plutôt réduite de l'autorité de contrôle[103].

Il est donc proposé d'instituer un directoire. Ce modèle garantit des prises de décision rapides, une bonne circulation des informations au sein de l'autorité, et s'accorde bien avec la création d'un comité spécialisé pour les bonnes pratiques ou les règles contraignantes (cf. ch. 4.1.2, let. b, et ch. 4.10.2, let. c). Les avantages liés à l'institution d'une autorité collégiale sont par ailleurs en grande partie conservés (indépendance, acceptation politique des décisions et sanctions).

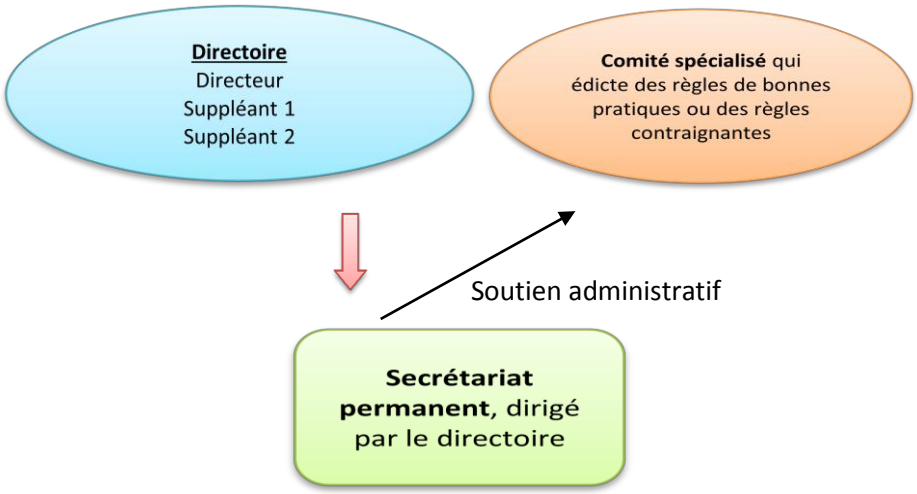
Le directoire serait composé d'un directeur et de deux suppléants, tous trois indépendants, et nommés par le Conseil fédéral, sous réserve de l'approbation de l'Assemblée fédérale. Le directoire dirigerait un secrétariat permanent qui lui assurerait un soutien administratif, préparerait ses décisions, conduirait les investigations et prendrait les décisions de procédure. Les décisions importantes devraient être prises par le collège.

L'autorité de contrôle aura peut-être à l'avenir des tâches et des compétences encore plus variées dans le domaine de la protection et dans celui de la transparence (surveillance avec pouvoir de décision [LPD] vs. médiation [art. 13 ss LTrans]). Pour éviter que ne montent au créneau ceux qui estiment qu'aujourd'hui déjà l'organisation du PFPDT conduit à des conflits d'intérêts et à un affaiblissement de la transparence, on pourrait envisager qu'un suppléant dirige l'unité consacrée à la protection des données et l'autre celle qui est dédiée à la transparence, sur le modèle de l'autorité de contrôle du canton de Fribourg (art. 29a de la loi du 25 novembre 1994 sur la protection des données; RSF 17.1)[104] . Les cas de conflits entre la protection des données et la transparence pourraient être tranchés par le directoire, qui pourrait dire ce qui prévaut dans le cas d'espèce.

---

[103] Voir le rapport du Conseil fédéral sur le gouvernement d'entreprise, FF 2006 7799 ss, 7834: « La forme organisationnelle de la commission doit être réservée aux entités nécessitant une certaine indépendance politique pour l'exécution de leurs tâches, mais pour lesquelles l'octroi de l'autonomie juridique n'est pas conseillé au niveau de l'entité (p. ex. en raison d'une taille insuffisante) ni au niveau du regroupement de plusieurs entités (p. ex. en raison d'interdépendances indésirables ou d'absence de potentiel de synergies).»

[104] Voir pour un organigramme: http://www.fr.ch/atprd/fr/pub/presentation/organisation.htm



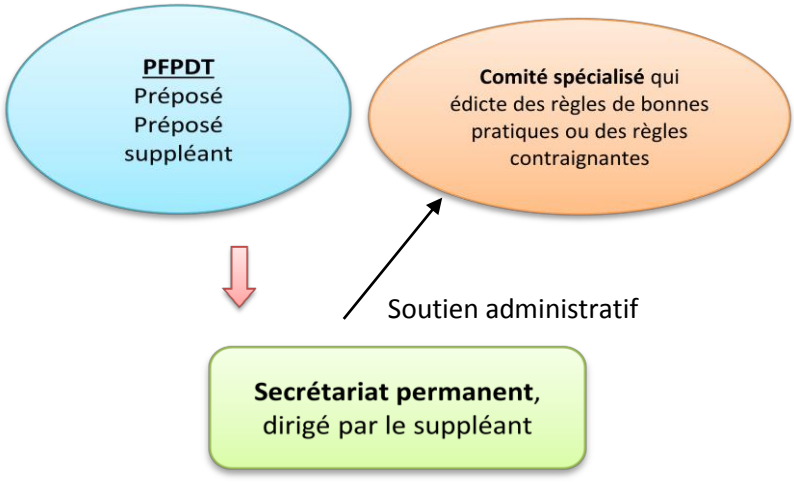
b) Autorité collégiale sans comité

Comme mentionné plus haut, *une minorité du groupe d'accompagnement* s'oppose à la création d'un comité spécialisé pour adopter/avaliser les règles de bonnes pratiques ou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.1.2, let. b, et ch. 4.10.2, let. c). Elle estime que cela ne ferait que créer des charges administratives supplémentaires et affaiblirait au final la protection des données. Dans le cas de l'autorité collégiale sans comité spécialisé, l'élaboration et/ou l'approbation des règles de concrétisation serait assurée pas l'un des trois membres du directoire.

c) Maintien du système actuel avec comité

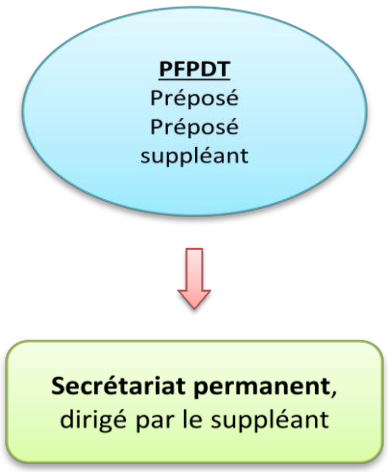
Le maintien du système actuel a pour avantage d'être simple et peu bureaucratique, et de garantir des réactions rapides de l'autorité de contrôle. On le connaît et on sait qu'il fonctionne. Le modèle du Préposé n'est au surplus pas rare. La majorité des cantons suisses a opté pour ce système, de même que de nombreux pays européens, tels l'Allemagne, le Royaume-Uni, la Hongrie, la Slovénie (sous le titre de « commissaire »), l'Espagne et la Pologne (sous le titre de « directeur »).

Pour renforcer l'indépendance de l'autorité de contrôle, il est proposé que le Préposé suppléant soit, comme le Préposé, aussi nommé par le Conseil fédéral moyennant accord de l'Assemblée fédérale.



d) Maintien du système actuel, sans comité

Comme mentionné plus haut, une *minorité du groupe d'accompagnement* s'oppose à la création d'un comité spécialisé pour adopter/avaliser les règles de bonnes pratiquesou les règles contraignantes à l'intention des auteurs de traitements (voir ch. 4.10.3, let. b, ci-dessus). Dans le cas du Préposé sans comité, l'élaboration et/ou l'approbation des règles de concrétisation serait assurée l'autorité de contrôle elle-même.



4.10.4 Renouvellement des rapports de fonction

Quel que soit le modèle d'organisation retenu, le groupe d'accompagnement propose de limiter le nombre de périodes de fonction des membres de l'autorité de contrôle à trois. Il estime que cela pourrait contribuer à leur indépendance et ouvrirait des perspectives de carrière, motivant ainsi des personnes qualifiées à postuler.

4.10.5 Collaboration entre autorités au plan national et international

En cas d'extension du champ d'application de la LPD aux traitements de données par les organes cantonaux, il aurait été opportun d'institutionnaliser et de renforcer la collaboration entre l'autorité de contrôle fédérale et les autorités cantonales. Puisque le groupe d'accompagnement a renoncé à une telle extension (ch. 4.2.1, let. a), il lui semble que la situation actuelle, basées principalement sur des échanges volontaires, ponctuels et informels, peut être maintenue.

Il faudra en revanche examiner la question de l'introduction de règles de coordination entre l'autorité de contrôle fédérale et les autorités cantonales, en cas de conflit de compétences positifs par exemple. Il faudra également examiner l'opportunité d'introduire des règles de coopération entre l'autorité de contrôle fédérale et les autorités de contrôle étrangères.

4.10.6 Financement

Le groupe d'accompagnement s'est penché sur la question de savoir comment les éventuelles nouvelles tâches de l'autorité de contrôle seraient financées. Il est en effet à prévoir que ces dernières, en particulier celles découlant du renforcement et de l'extension des attributions de l'autorité de contrôle, entraîneront un besoin en ressources supplémentaires (cf. ch. 4.10.2).

Une majorité du groupe d'accompagnement est d'avis qu'il faut mettre davantage de moyens financiers à la disposition de l'autorité de contrôle. Elle estime que ce financement doit continuer à être assuré par le biais du budget ordinaire de la Confédération, c'est-à-dire des recettes fiscales générales.

Une minorité du groupe d'accompagnement propose en revanche l'introduction d'une taxe comme source de financement supplémentaire. L'obligation de verser cette dernière pourrait être réglée de façon analogue à celui prévu par la législation britannique [105]; le traitement commercial de données électroniques serait soumis à enregistrement, lui-même soumis au paiement d'une taxe (dont le montant dépendrait par exemple de la taille de l'entreprise). Plusieurs membres du groupe d'accompagnement considèrent que cette solution entraînerait une importante charge administrative, serait difficile à mettre en œuvre dans un contexte international et pourrait entraîner une répercussion des frais sur le consommateur. En outre, il faudrait étudier plus en détail si l'introduction d'une telle taxe nécessite une base constitutionnelle. Cela dépend si l'on qualifie cette taxe d'impôt ou de contribution causale. Pour percevoir un impôt, la Confédération a besoin d'une compétence expresse et spécifique inscrite dans la Constitution fédérale. Une simple compétence matérielle ne suffit en règle générale qu'à justifier la perception d'émoluments ou de charges de préférence (contributions causales classiques), de taxes d'incitations à proprement parler ou de taxes s'en approchant. Le critère principal pour distinguer un impôt d'une contribution causale est celui de l'imputabilité. On parle d'impôt lorsque l'assujetti doit s'acquitter d'une contribution sans que l'État ne fournisse une contre-prestation qui lui profite individuellement (inconditionnalité de la contribution)[106]. Si l'on devait aménager une taxe pour financer les tâches de l'autorité de contrôle, il faudrait en particulier définir pour quelles activités de l'autorité de contrôle ou pour quelle(s) affectation(s) ces montants sont perçus, et qui y est assujetti.

Une réglementation telle que la connaît la Grande-Bretagne devrait vraisemblablement être considérée en Suisse comme un émolument administratif, ne requérant pas de base constitutionnelle. Cette taxe serait cependant limitée par les principes de la couverture des frais et de l'équivalence. Autrement dit, elle ne pourrait guère dépasser les frais administratifs liés à l'enregistrement et ne pourrait donc pas servir au financement d'autres tâches de l'autorité de contrôle. Il serait envisageable, à certaines conditions, de renoncer à la base constitutionnelle aussi pour la taxe de surveillance – à l'instar du cas de la surveillance des banques et des assurances privées – si le cercle des assujettis (p. ex. auteurs commerciaux de traitements de données électroniques) coïncidait avec delui des bénéficiaires de la redevance. Le montant devrait alors être fixé de manière à couvrir les frais du contrôle des assujettis (p.

---

[105] Le modèle britannique repose sur un enregistrement obligatoire des entreprises. En vertu du « Data Protection Act 1998 », tout « Data Controller » (en particulier des entreprises et des entreprises individuelles) doit s'enregistrer auprès de l'autorité de contrôle britannique, ICO. Des exceptions sont toutefois prévues. Les frais de la « Data Protection Registration » sont déterminés en fonction de la taille et du chiffre d'affaires de l'entreprise. Pour la plupart des entreprises, ils se montent à 35 livres. A partir d'une certaine valeur-seuil (chiffre d'affaires supérieur à 25,9 millions de livres et plus de 249 employés), la taxe atteint 500 livres. Pour les autorités étatiques comptant plus de 249 employés, les frais sont également de 500 livres. Voir à ce propos <http://ico.org.uk/for_organisations/data_protection/registration>.

[106] Voir l'expertise détaillée l'OFJ du 19 juillet 1999, in : VPB 2000, N° 25 (en allemand avec résumé en français). Dans ce document, l'OFJ a défendu une position un peu moins stricte, selon laquelle une base constitutionnelle explicite et spécifique est requise pour le prélèvement de telles redevances lorsqu'il n'y pas de lien d'imputation entre le cercle des assujettis et l'affectation de la redevance ou lorsque l'intensité de ce lien est trop faible (ch. A/III./1./b). S'agissant de la perception annuelle de taxes forfaitaires dans le domaine de la surveillance des banques et des assurances privées ainsi que de la prévention des accidents de la route, l'OFJ a conclu qu'il devait y avoir congruence entre le cercle des assujettis et le cercle de personnes qui bénéficient, comme groupe, de l'utilisation de ces fonds. Il lui paraissait par conséquent acceptable que les taxes de surveillance et la contribution à la prévention des accidents soient fondées sur la compétence matérielle de la Confédération dans les domaines concernés et qu'il soit renoncé à une base constitutionnelle explicite et spécifique pour ces redevances.

ex. auteurs commerciaux de traitements de données électroniques). Les frais de surveillance des autres auteurs de traitements (p. ex. auteurs privés et non commerciaux de traitements, organes fédéraux) ne pourraient par contre pas être couverts par une telle taxe (sans base constitutionnelle ad hoc). Un tel système serait très complexe dans sa mise en œuvre et générerait de nouveaux investissements en personnels et financiers.

Le groupe d'accompagnement a également examiné un modèle (appliqué en Espagne p. ex.) où les recettes du budget proviennent des amendes prononcées par l'autorité de contrôle, mais il l'a rejeté pour plusieurs raisons. Tout d'abord, il n'a pas encore été décidé si l'autorité de contrôle sera investie de compétences de prononcer des sanctions pécuniaires et, dans l'affirmative, si ces dernières permettraient de générer suffisamment de rentrées (cf. ch. 4.10.2). Ensuite, la majorité du groupe d'accompagnement est d'avis qu'une telle approche serait en contradiction avec les principes de la politique financière. Enfin, il ne faut pas que l'on ait l'impression que l'autorité de contrôle prononce des sanctions pour s'autofinancer.

Pour renforcer l'indépendance de l'autorité de contrôle, le groupe d'accompagnement propose de lui octroyer une compétence budgétaire similaire à celle du Contrôle fédéral des finances[107]. La conséquence serait que le budget de l'autorité de contrôle serait soumis directement au Parlement (sans modification par le Conseil fédéral).

4.11 Dispositions pénales

La LPD contient actuellement deux dispositions pénales, les art. 34 et 35. D'autres dispositions figurent dans le code pénal aux art. 179 ss CP, soit dans la partie consacrée aux infractions contre le domaine privé ou secret. Il s'agit d'examiner si ces articles, compte tenu notamment des développements technologiques (drônes, Google Glasses, Dashcams, etc.) doivent être maintenus tels quels, doivent être renforcés (p. ex. en en faisant des infractions poursuivies d'office), ou encore s'il convient d'en créer d'autres.

Une partie des membres du groupe d'accompagnement estime qu'il faut introduire dans le code pénal une disposition concernant l'usurpation d'identité. Il est dans un premier temps proposé d'attendre de voir si le Conseil national donne suite ou non à la motion Comte 14.3288 « Faire de l'usurpation d'identité une infraction pénale en tant que telle », dont le Conseil fédéral proposait le rejet, mais qui a été acceptée par le Conseil des États le 12 juin 2014[108].

4.12 Dispositions finales

Les dispositions relatives aux compétences législatives du Conseil fédéral (art. 36 LPD) et à l'exécution par les cantons (art. 37 LPD) doivent être adaptées aux modifications décrites aux ch. 4.1 à 4.11. Enfin, il faut prévoir des dispositions transitoires pour les innovations proposées (cf. art. 38 LPD).

5. Forme de l'acte normatif et contexte normatif

Bases constitutionnelles : la Constitution fédérale ne contient aucune disposition attribuant expressément à la Confédération une compétence législative dans le domaine de la protec-

---

[107] Voir art. 2, al. 3, de la loi sur le Contrôle des finances (LCF, RS 614.0).

[108] Lors de sa séance du 17 octobre 2014, la Commission des affaires juridiques du Conseil national a recommandé, par 19 voix contre 1, l'adoption de la motion Compte 14.3288.

tion des données[109]. En revanche, certaines compétences fédérales englobent la faculté pour la Confédération d'édicter aussi des dispositions en matière de protection des données. Dans le secteur privé, le législateur peut notamment s'appuyer sur sa compétence législative dans le domaine du droit civil (art. 122 Cst.)[110]. Dans le domaine du droit public, la compétence de la Confédération d'édicter des dispositions de protection des données applicables à l'administration résulte de son pouvoir d'organisation selon l'art. 173, al. 2, Cst. La Confédération n'a en revanche pas la compétence d'édicter des dispositions sur la protection des données pour les administrations cantonales et communales[111],[112]. Les mesures prévues au ch. 4 de la présente esquisse d'acte normatif peuvent, selon le groupe d'accompagnement, être fondées sur les bases constitutionnelles existantes. Une révision partielle de la Constitution serait toutefois requise si :

- la répartition des compétences entre Confédération et cantons dans le domaine de la protection des données devait être modifiée et si le champ d'application de la LPD devait être étendu aux organes cantonaux (cf. ch. 4.2.1, let. a, où il est toutefois proposé de renoncer à une telle mesure) ; et
- une taxe prenant la forme d'un impôt devait être introduite pour financer les tâches de l'autorité de contrôle (cf. ch. 4.10.6).

Réglementation aux niveaux de la loi et de l'ordonnance : les adaptations proposées au ch. 4 visent essentiellement la révision de la LPD elle-même. Vu que plus de la moitié de ses dispositions seront touchées, une révision totale de la loi est indiquée.

Une révision de la loi nécessitera une adaptation des ordonnances d'exécution (OLPD, OCPD). Il se peut que des modifications ponctuelles soient nécessaires aussi dans des lois procédurales (CPC, PA, LTAF, LTF). En outre, une révision de la LPD impliquera de vérifier si les dispositions de protection des données contenues dans des lois spéciales (cf. ch. 4.1 et 4.9.1) satisfont encore aux nouvelles exigences de la LPD. Enfin, il faudra examiner la nécessité de modifier les dispositions pénales sur la protection de la sphère secrète et privée (en particulier les art. 179 ss CP) (cf. ch. 4.11).

Droit international : les travaux de révision de la LPD doivent prendre en compte les réformes en cours en matière de protection des données au Conseil de l'Europe et dans l'UE. Ils doivent en particulier créer les conditions nécessaires à une éventuelle ratification de la Convention STE 108 modernisée (cf. le ch. 2 à ce propos).

---

[109] L'art. 13, al. 2, Cst. stipule certes que « toute personne a le droit d'être protégée contre l'emploi abusif des donées qui la concernent ». Mais il s'agit ici d'un droit fondamental, qui ne confère aucune compétence à la Confédération. Une révision de cette disposition constitutionnelle fait d'ailleurs l'objet de l'initiative parlementaire Vischer 14.413 « Droit fondamental à l'autodétermination en matière d'information », qui vise la modification de l'art. 13, al. 2, Cst. de sorte « à faire de la protection des données un droit fondamental à l'autodétermination en matière d'information au lieu d'un droit à la protection contre les abus ». La Commission des institutions politiques du Conseil national (CIP-CN) a donnée suite à cette initiative parlementaire le 29 août 2014.

[110] D'autres normes constitutionnelles pertinentes sont par exemple l'art. 95 Cst. (compétence de la Confédération pour légiférer sur l'activité économique lucrative privée) et l'art. 97 Cst. (compétence de la Confédération en matière de protection des consommateurs).

[111] Sous réserve des cas dans lesquels les cantons traitent des données en exécution du droit fédéral (cf. art. 37 LPD).

[112] Cf. le message du Conseil fédéral du 19 février 2003 relatif à la révision de la loi sur la protection des données (LPD), FFI 2003 1915, 1961 s.

6. Structure générale de la réglementation

Le groupe d'accompagnement propose de maintenir pour l'essentiel la structure de l'actuelle LPD et de la compléter là ou cela est nécessaire (cf. ch. 4). La nouvelle loi comprendrait vraisemblablement plus d'articles et contiendrait des dispositions :

- relatives au but, au champ d'application et aux définitions ;
- générales sur la protection des données, applicables aussi bien aux organes de la Confédération qu'aux privés (principes du traitement de données, droits des personnes concernées, communication transfrontière, procédures de certification) ;
- relatives au traitement de données par des particuliers (états de fait portant atteinte à la personnalité, motifs justificatifs, dispositions procédurales)
- relatives au traitement de données par des organes fédéraux (en particulier exigence de bases légales suffisantes pour le traitement, dispositions de traitement spécifiques, dispositions procédurales) ;
- relatives à l'organisation et aux tâches de l'autorité de contrôle ;
- relatives à la procédure de contrôle ;
- relatives au mode alternatif de règlement des litiges et à la création d'un organe de médiation ;
- relatives au comité chargé d'édicter ou d'approuver les réglementations de détail concernant l'application de la LPD ou les règles de bonnes pratiques ;
- pénales ; et
- finales (exécution, dispositions transitoires).

7. Densité normative (degré de détail)

La loi sur la protection des données est conçue de manière technologiquement neutre. Elle contient surtout des règles de fond qui sont valables pour toute utilisation de données personnelles. Il faudra par conséquent éviter une trop grande spécialisation et une trop grande précision. Les principes généraux de traitement des données doivent en particulier être formulés de manière assez abstraite afin de laisser aux autorités une marge de manœuvre suffisante. Le groupe d'accompagnement propose par conséquent de maintenir l'actuelle densité normative de la LPD.

Pour améliorer la mise en œuvre de la loi et la sécurité du droit, le groupe d'accompagnement estime qu'il faut d'avantage concrétiser le droit de la protection des données à un autre niveau réglementaire. Il est ainsi prévu de préciser la LPD par le biais de bonnes pratiques ou de dispositions réglementaires plus détaillées (ch. 4.1.2, let. b). Une majorité du groupe d'accompagnement est d'avis que ce but peut être atteint au moyen de règles de bonnes pratiques non contraignantes. Ces règles devraient être établies ou approuvées par un comité d'experts (cf. 4.1.2, let. b, 4.10.2, let. c, et 4.10.3).

8. Calendrier

Le Conseil fédéral a chargé le DFJP de lui soumettre, d'ici à la fin de 2014, des propositions sur la suite des travaux pour une éventuelle révision de la LPD. À cet effet, l'OFJ va élaborer – en tenant compte de la présente esquisse d'acte normatif – une note de discussion à l'intention du Conseil fédéral. Étant donné que le CAHDATA achèvera vraisemblablement ses travaux concernant le projet de modernisation de la Convention STE 108 en décembre

2014 (cf. ch. 2), il pourrait être judicieux de ne soumettre la note de discussion au Conseil fédéral qu'au début de 2015, de manière à ce que les résultats au sein du Conseil de l'Europe puissent être pris en compte dans le processus de prise de décision.

La note de discussion doit répondre à des questions fondamentales sur le contenu et proposer un calendrier pour la suite des travaux. Pour ce dernier, le groupe d'accompagnement envisage trois options :

- Attendre que les réformes européennes dans le domaine de la protection des données soient terminées avant d'entamer la révision de la LPD.
- Charger le DFJP d'élaborer un avant-projet de révision de la LPD sans attendre la fin des travaux de réforme européens.
- Charger le DFJP d'élaborer un avant-projet de révision de la LPD, en prévoyant un délai suffisamment long (p. ex. deux ans) afin que l'on sache quelles adaptations du droit suisse sur la protection des données sont nécessaires pour une ratification de la Convention STE 108 modernisée et qu'il puisse en être tenu compte.

Annexe : prises position de certains membres du groupe d'accompagnement

economiesuisse

per Mail
Frau Monique Cossali Sauvain
Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz (BJ)
Direktionsbereich Öffentliches Recht
Fachbereich Rechtsetzungsprojekte und -methodik
Bundesrain 20
3003 Bern

23. September 2014

Stellungnahme economomiesuisse zum Normkonzept Revision Datenschutzgesetz (DSG)

Sehr geehrte Frau Cossali

Sie haben uns eingeladen, zum Normkonzept zur Revision Datenschutzgesetz (DSG) (Fassung vom 10. September 2014) Stellung zu nehmen, falls wir dies wünschen. Für die gebotene Gelegenheit zur Meinungsäusserung danken wir Ihnen bestens und machen nachfolgend gerne davon Gebrauch. Zu diesem Zeitpunkt beschränken wir uns dabei auf die wichtigsten Punkte mit grundlegendem Charakter und ohne einen Anspruch auf Vollständigkeit zu erheben.

Ein funktionierender Datenschutz ist aus Sicht der Wirtschaft wichtig

Die Diskussion über den Datenschutz ist vor dem Hintergrund des technologischen Wandels angebracht und muss geführt werden. **Für die Wirtschaft ist ein angemessenes und wirksames Datenschutzgesetz wichtig. Massvolle und klare Bestimmungen lassen Raum für die wirtschaftliche Entfaltung und dienen der Rechts- und Investitionssicherheit. Sie ermöglichen die Entwicklung und den Einsatz von innovativen digitalen Produkten und industriellen Anwendungen.**

Darüber hinaus sind Akzeptanz und Vertrauen der Nutzer in den Datenschutz eine zentrale Voraussetzung für die Fortentwicklung der immer wichtiger werdenden digitalen Wirtschaft und die Nutzung des damit verbundenen wirtschaftlichen Potenzials. Der überwältigende Teil der Unternehmen hat denn auch ein grosses Interesse daran, dass datenschutzrechtliche Vorschriften eingehalten werden – nicht nur im eigenen Haus, sondern auch durch die anderen Wettbewerber. Andernfalls drohen massive Reputationsschäden, die nicht nur die unmittelbar betroffenen Unternehmen belasten, sondern gleich ganze Branchen in Mitleidenschaft ziehen können. Ausserdem besteht das Risiko, dass nicht datenschutzkonforme Produkte, Dienstleistungen und ganze Geschäftsmodelle nachträglich verboten werden und damit bereits getätigte Investitionen verloren gehen.

economiesuisse
Hegibachstrasse 47
Postfach CH-8032 Zürich
Telefon +41 44 421 35 35
Telefax +41 44 421 34 34

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

Intelligente Datenschutzvorschriften, die ein gutes Datenschutzniveau bieten, sind für die Unternehmen und für den Wirtschaftsstandort Schweiz ein Vorteil. Überschiessende und im Geschäftsalltag nicht praktikable Regulierungen wirken sich hingegen innovationshemmend aus und können der Wettbewerbsfähigkeit von Unternehmen im internationalen Umfeld schaden. Sie treffen ebenso die Nutzer, die nicht von neuen Produkten und Dienstleistungen profitieren können. Nicht umsonst heisst es denn auch in der Botschaft zum geltenden DSG, dass die durch die immer besseren Technologien ermöglichte Entwicklung nicht verhindert oder eingeschränkt werden soll (Bundesrat / BBl 1988 II 417). Diese Feststellung gilt uneingeschränkt auch für die Gegenwart.

Bei einer geplanten DSG-Revision ist auch zu beachten, dass beim Datenschutzrecht, das eine Konkretisierung des Grundrechts zum Schutz auf Privatsphäre (Art. 13 BV) darstellt, der Schutzaspekt im Verhältnis *zwischen Staat und Bürger* die höchste Bedeutung ist. Demgegenüber ist das Verhältnis *zwischen Privaten* vom Grundsatz der Privatautonomie geprägt, weshalb in diesem Bereich übermässige Datenschutzregulierungen besonders problematisch und rechtfertigungsbedürftig sind und nur mit Zurückhaltung erlassen werden dürfen. Der Nutzen, den die sich verbessernden Informationstechnologien bieten, soll nicht leichtfertigt geopfert werden. Jeder Einzelne soll im Privatbereich grundsätzlich selbst entscheiden können, ob er ein bestimmtes (allenfalls mit einer Bekanntgabe gewisser Daten verbundenes) Angebot nutzen möchte oder nicht. Als mündiger Bürger ist er dazu auch ohne weiteres in der Lage.

Weiter gilt es auch im Blick zu behalten, dass Datenschutzrecht nicht Konsumentenrecht ist. Die beiden Bereiche verfolgen unterschiedliche Schutzzwecke und sollen folglich nicht vermischt werden: Während das erste nämlich auf den Grundrechtschutz ausgerichtet ist; bezieht sich das zweite auf kommerzielle Beziehungen zwischen Anbietern und Abnehmern. Daher haben etwa Instrumente wie Sammelklagen oder vom allgemeinen haftpflichtrechtlichen Regime abweichende Schadenersatzklagen etc. keinen Platz im DSG.

<u>Grundsätzliche Bemerkungen zum gesellschaftspolitischen Umfeld und zum Revisionsprojekt DSG</u>

In den letzten Jahren ist die Präsenz des Themas Datenschutz in den Medien und der öffentlichen Wahrnehmung gestiegen, und es hat in der politischen Agenda an Bedeutung gewonnen. Das hat verschiedene Gründe: Zum einen haben spektakuläre Überwachungs- und Spionageaffairen und das Bekanntwerden schwerwiegender Eingriffe in die Privatsphäre der Bürger durch geheimdienstliche Behörden die Sensibilität für den Datenschutz erhöht (obschon es hier eigentlich nicht um Probleme des Datenschutzes sondern vielmehr der Datensicherheit geht). Sie haben teilweise auch ein diffuses Unbehagen gegenüber den Möglichkeiten, die mit den neuen Informations- und Kommunikationstechnologien einhergehen, hervorgerufen. Dieser Eindruck wird zusätzlich verstärkt durch Meldungen über Hackerattacken und Datendiebstahl bzw. -verluste bei einzelnen grossen in- und ausländischen Unternehmen. Weiter hat mit den verbesserten Bearbeitungsmöglichkeiten und höheren Speicherkapazitäten die Menge der verarbeiteten Daten zugenommen. Gleichzeitig entstehen zahlreiche neue internetbasierte Geschäftsmodelle und Anwendungen, und die Sozialen Medien erleben einen regelrechten Boom. Mit diesen Entwicklungen gehen auch Fragen betreffend den (zu leichtfertigen) Umgang mit persönlichen Daten einher. Zudem ergingen einige vielbeachtete letztinstanzliche Grundsatzentscheide zu relevanten datenschutzrechtlichen Fragen, die eine Handvoll besonders technologienaher Unternehmen betrafen (vgl. die Bundesgerichtsentscheide betreffend Logistep und Google Street View oder das EuGH-Google-Urteil betreffend Löschungsrecht).

So notwendig die Diskussion um den Datenschutz in diesem sich verändernden gesellschaftlich-technologischen Umfeld ist, so essentiell ist es mit Blick auf eine mögliche Revision des DSG, dass

das bewährte heutige Datenschutzregime nicht ohne Notwendigkeit und zeitliche Dringlichkeit über den Haufen geworfen wird; vor allem Im Privatbereich. **Bevor eine Revision an die Hand genommen wird, müssen zwingend der tatsächliche Handlungsbedarf anhand von Fakten und empirischen Untersuchungen konkret ausgewiesen sowie das angestrebte Ziel klar definiert sein. Es ist transparent und detailliert aufzuzeigen, inwiefern genau die geltenden Regelungen ihre Wirkung verfehlen und ob bzw. mit welchen Mitteln ein allfälliger Missstand effektiv behoben werden kann.** Nur so lassen sich die verschiedenen Alternativen (inklusive eines „Nichtstuns“) abschätzen. Und nur so lassen sich die Interessen gegeneinander abwägen und ausgleichen, und lässt sich die Verhältnismässigkeit von neu vorgeschlagenen Vorschriften überprüfen. Diese Kriterien sind beim laufenden Revisionsprojekt jedoch nicht erfüllt.

Darüber hinaus darf eine Revision auch nicht nur auf einige wenige vielbeachtete Einzelfälle bzw. auf eine Branche oder gar ein paar wenige internationale Konzerne gemünzt sein. Denn **das DSG gilt für die gesamte Wirtschaft – für alle Industriezweige, grosse und kleine, national wie international tätige Unternehmen. Durch unpassende Regulierungen, die ihr eigentliches Ziel verfehlen oder darüber hinausschiessen, werden alle Unternehmen getroffen. Deshalb muss sich eine Revision auf die wesentlichen Punkte beschränken auf einer konkreten und detaillierten Risikoanalyse aufbauen. Dabei sind die angeblichen Lücken genau aufzuzeigen, und es ist zu benennen, was die Folge einer Nichtregelung im Privatbereich wäre.**

Fehlender Handlungsbedarf für eine umfassende DSG-Revision

Der Bedarf für eine umfassende DSG-Revision ist nach wie vor nicht konkret bzw. unzureichend ausgewiesen. Nur sechs Jahre nach der letzten Revision braucht es für den Privatbereich keine neuerliche Überarbeitung des Gesetzes, die über formelle Anpassungen wie z.B. eine übersichtlichere Darstellung oder allenfalls einzelne punktuelle Verbesserungen hinausgeht. Allein der Umstand, dass sich das technologische und gesellschaftliche Umfeld weiterentwickelt, ist jedenfalls kein Anlass, von einem funktionierenden System abzuweichen. Das DSG wurde bewusst technologieneutral ausgestaltet, und es hat sich seither bestens bewährt. economiesuisse lehnt daher eine Revision in der vorgesehenen Form ab. Insbesondere sehen wir nicht, wo und inwiefern beim geltenden Recht Mängel bestehen sollten, die einen so weitgehenden gesetzgeberischen Eingriff erforderlich machen würden.

Ziel der 2010 im Auftrag des Bundsamts für Justiz (BJ) durchgeführten Evaluation des DSG war es, das DSG auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund standen erstens die Bekanntheit und die Durchsetzungsmechanismen des Gesetzes einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits. Der Schlussbericht zur Evaluation vom 9. Dezember 2011 weist zusammenfassend auf die technologische Entwicklung als Herausforderung hin (S. I), er stellt aber keine schweren Mängel fest. Vielmehr hält als Gesamtbilanz fest, dass der EDÖB seinen gesetzlichen Auftrag erfülle und dabei eine hohe Wirksamkeit erziele und seine Aufsichtstätigkeit im Einzelfall wirksam sei: In der Mehrheit der Sachverhaltsabklärungen stelle er nur geringfügige Probleme fest, welche die Datenbearbeiter anschliessend freiwillig behöben. Spreche er bei grösseren Mängeln Empfehlungen aus, würden diese grossmehrheitlich umgesetzt, entweder direkt oder nach einem Gerichtsurteil. Bei Bearbeitungen, die intransparent sind oder im Ausland erfolgen, stosse die Aufsicht an Grenzen. Zudem mache der EDÖB heute aus Ressourcengründen keine stichprobenartigen Kontrollen, was der Breitenwirkung der Aufsicht abträglich sei. Mit einer präventiven Wirkung auf andere Datenbearbeiter sei aber insofern zu rechnen, als bekannt werdende Missstände öffentliches Interesse erregen (S. III f.). Es gebe auch deutliche Hinweise, dass das Risiko eines Imageschadens das Verhalten zugunsten des Datenschutzes beeinflusst (S. II). Auch die Beratungs- und Informationstätigkeit würden von den

Bearbeitern insgesamt als nützlich, praxisnah und konstruktiv bewertet (S. III f.). Bezüglich des Verhaltens der Nutzer hält der Bericht fest, dass die Betroffenen die neuen Möglichkeiten der Informationsgesellschaft mehrheitlich begrüssten (S. 66). Sie erachteten Datenschutz zwar als wichtig, schützten sich aber nicht immer konsequent selbst und gäben persönliche Daten bisweilen grosszügig preis. Betreffend die Schutzrechte gelangt der Bericht zum Schluss, dass die im DSG verankerten Durchsetzungsrechte der Betroffenen im internationalen Rechtsvergleich gut ausgebaut seien sowie dass Betroffene den Rechtsweg selten beschritten (S. II). Das Fazit des Berichts lautet: Vom DSG gehen klare Wirkungen zugunsten des Datenschutzes aus. Gleichzeitig sind die Wirkungen des EDÖB in verschiedener Hinsicht begrenzt und die Betroffenen machen wenig Gebrauch von den vorhandenen Durchsetzungsrechten (S. IV). Über die Gründe hierfür kann im Bericht nur spekuliert werden: Als mögliche Erklärung wird „erstens die vermutlich geringe Bekanntheit der Durchsetzungsrechte und des Rechtswegs sowie das geringe Wissen über die Anwendung dieser Rechte" genannt. Und zweitens „dürfte aus Sicht der Betroffenen ein vergleichsweise beträchtlicher Aufwand einer Klage einem diffusen und nicht gesicherten Nutzen gegenüberstehen" (S. II f.).

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 zur Evaluation des DSG drängt sich kein dringender Handlungsbedarf auf, weder in inhaltlicher noch zeitlicher Hinsicht. Insbesondere lässt sich aus dem Papier nicht herleiten, dass das DSG seine bzw. die gewünschte Schutzwirkung nicht entfalte. Ebenso wenig legt es nahe, dass etwa die Durchsetzungsrechte oder die Kompetenzen der Aufsichtsbehörde zu schwach wären und daher ausgebaut werden sollten oder gar müssten. Vielmehr hält der Bericht fest, dass es in einem weiteren Schritt Aufgabe der Politik sei zu entscheiden, ob eine umfassende Diskussion über den Datenschutz geführt werden soll und welches das gewünschte Schutzniveau des DSG sein solle (S. IV, S. 215). So werden im Bericht denn auch ausdrücklich nicht Empfehlungen ausgesprochen, sondern mögliche Handlungsoptionen angedacht. Diese (teilweise sehr einschneidenden) Optionen haben „eher der Charakter von Gedankenanstössen als derjenige eines Arbeitspapiers im Hinblick auf die Formulierung im Einzelnen analysierter Vorschläge" (S. 215, 217).

economiesuisse fordert, dass keine umfassende DSG-Revision wie die geplante in Angriff genommen wird, ohne dass angebliche Missstände unter dem geltenden DSG klar belegt sind. Hierbei muss auf Fakten abgestellt werden. Gesetzgeberischer Aktivismus, getrieben von einem unbestimmten Misstrauen gegenüber dem veränderten technologischen Umfeld und ausgehend von Stimmungen oder blosse Vermutungen, ist verfehlt. So kann etwa aus der Tatsache, dass die Nutzer selten den Rechtsweg beanspruchen, keineswegs automatisch auf Defizite des DSG geschlossen werden. Die geringe Beanspruchung der Gerichte sehen wir im Gegenteil als Hinweis darauf, dass das heutige Datenschutzsystem seinen Zweck erfüllt. So lieferten denn auch etwa die Fälle Logistep, Google Streetview oder Moneyhouse – die gerne als Beispiele für die mit den neuen Technologien verbundenen Problematiken angeführt werden – keinerlei Hinweise darauf, dass im geltenden Recht etwa die Klagerechte zu schwach ausgestaltet wären, Beweisschwierigkeiten bestünden, die Kompetenzen des EDÖB zu wenig weit reichten oder Sanktionsmöglichkeiten fehlten. Vielmehr ging es in diesen Fällen jeweils um Auslegungsfragen des DSG, in denen die angerufenen Gerichte Klarheit schafften.

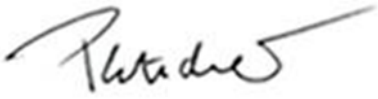
<u>Anpassung an internationale Bestrebungen (EU/Europarat) nur sofern für Marktzugang zwingend</u>

Das durch das geltende DSG garantierte Schutzniveau ist im internationalen Vergleich bereits hoch; eine Verschärfung insbesondere im Privatbereich ist unnötig. Ein überzogenes, „veradministriertes" Datenschutzrecht würde die Schweiz global gesehen ins Hintertreffen bringen. Dabei darf sich der Vergleich nicht allein an Europa orientieren, sondern der Blick ist darüber hinaus insbesondere auch auf die USA und Asien zu richten. Ein im Verhältnis zur EU schlank

ausgestaltetes, „smartes“ Datenschutzrecht ist ein willkommener Wettbewerbsvorteil für die Schweizer Wirtschaft.

Wenn überhaupt, besteht Handlungsbedarf aus Sicht von economiesuisse nur für den Fall und insoweit, als durch die Revisionen auf europäischer Ebene der Marktzugang zur EU betroffen ist. Bevor das Schweizer Recht erneut revidiert wird, sollten unbedingt zuerst die Resultate der laufenden Entwicklungen in der EU und im Europarat abgewartet werden. Eine allfällige Anpassung an das europäische Recht bzw. Umsetzung ins nationale Recht soll schliesslich nur dort erfolgen, wo dies unter dem Gesichtspunkt des Marktzugangs zwingend notwendig ist. Dazu muss bei jeder vorgeschlagenen Änderung nachvollziehbar sein, welches das unbedingte gesetzgeberische Minimum ist, um die Gleichwertigkeit mit dem europäischen Datenschutzstandard zu erfüllen. Hierbei ist zu bedenken, dass es keiner absoluten Gleichwertigkeit bedarf (vgl. die Safe-Harbor-Lösungen im Verhältnis CH/EU-USA). Der Schweizer Gesetzgeber darf auf keinen Fall überhastet und ohne ausgewiesene Notwendigkeit übertriebene Regelungen ungeprüft aus dem europäischen Umfeld übernehmen. Der vorhandene Spielraum ist weitestmöglich auszunützen.

Freundliche Grüsse
economiesuisse



Thomas Pletscher
Mitglied der Geschäftsleitung

Dr. Marlis Henze
Wissenschaftliche Mitarbeiterin

Dachorganisation der Schweizer KMU
Organisation faîtière des PME suisses
Organizzazione mantello delle PMI svizzere
Umbrella organization of Swiss SME

Aktennotiz

Geht an Bundesam für Justiz, Frau Monique Cossali, Leiterin der Belgeitgruppe DSG

Bern, 6. Oktober 2014 sgv-Kl

Stellungnahme des sgv zum Normkonzept zur Revision des Datenschutzgesetzes (DSG) (Version vom 10.9.2014)

Die vorliegende Stellungnahme bezieht sich auf das Normkonzept vom 10. September 2014 und erhebt keinen Anspruch auf Vollständigkeit. Sie gibt lediglich die Position des sgv in den wichtigsten Punkten wieder.

Grundsätzliche Bemerkungen

Die letzte grössere Revision des DSG liegt 6 Jahre zurück. Nach Ansicht des sgv ist es verfrüht, an den eben erst geschaffenen Grundlagen zu rütteln. Eine Revision des DSG rechtfertigt sich derzeit nicht. Zuerst sollen die Ergebnisse der Diskussionen in der EU und im Europarat abgewartet und dann allenfalls notwendige Anpassungen des DSG vorgenommen werden.

Aus dem Bericht des Bundesrates vom 9. Dezember 2011 wird nicht klar ersichtlich, wo genau eine Revision des DSG ansetzen soll. Ziel des Berichts war es gemäss Bundesrat, „das Datenschutzgesetz auf seine Wirksamkeit hin zu überprüfen. Im Vordergrund der Untersuchung standen die Bekanntheit des Gesetzes und seine Durchsetzungsmechanismen einerseits sowie die Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) andererseits“. Im Bericht wird festgehalten, dass die technologischen Entwicklungen das DSG herausfordern. Zudem würde es immer schwieriger, die Kontrolle über einmal bekannt gegebene Daten zu behalten. Aufgrund der Ergebnisse der Evaluation ist der Bundesrat der Auffassung, dass zu prüfen ist, inwieweit und in welcher Weise die Datenschutzgesetzgebung anzupassen ist, um den rasanten technologischen und gesellschaftlichen Entwicklungen Rechnung zu tragen. Aus dem Bericht wird klar, dass der EDÖB zusätzliche Ressourcen geltend macht.

Der Schweizerische Gewerbeverband sgv ist der Auffassung, dass die Öffentlichkeit gut informiert ist. Dafür sorgen nicht nur zahlreiche Publikationen von Konsumentenorganisationen, sondern z.B. auch die Webseite des EDÖB, von der sich jedermann nützliche Informationen zur Rechtslage herunterladen kann. Die Diskussion um social media und den Schutz der Persönlichkeit gegen den Missbrauch von grundsätzlich frei zugänglichen Daten ist berechtigt und notwendig. Sie darf aber nicht zum Aufbau einer weiteren Bürokratie führen.

Stellungnahme zu den Eckwerten des Normkonzepts (contenu essentiel de la révision)

4.1 Concept et mise en oeuvre

Der sgv unterstützt die Stossrichtung, dass das Datenschutzgesetz technologieneutral ist und sich auf die grundlegenden Prinzipien fokussiert. Da der Datenschutz sehr unterschiedliche Anforderungen haben kann, macht es Sinn, weiterhin sowohl ein allgemeines DSG als auch die spezialgesetzlichen Regelungen zu haben.

Allein aus der Tatsache, dass heute betroffene Personen ihre Rechte gegenüber Datenbearbeitern nur selten beanspruchen, nur wenige Betroffene Klage einreichen und Prozesse über datenschutzrechtliche Fragen führen, ist kein hinreichender Grund zur Stärkung der Kontrollbehörde. Die relativ geringe Zahl gerichtlicher Verfahren kann ebenso gut mit einem von der Öffentlichkeit insgesamt als

befriedigend empfundenen System erklärt werden. Dass heute die Nachfrage danach so klein ist, ist ein deutliches Zeichen dafür, dass kein Handlungsbedarf besteht. Eine Stärkung des Datenschutzbeauftragten drängt sich aus Sicht des sgv im heutigen Zeitpunkt nicht auf. Neue gesetzliche Vorschriften sind nicht notwendig. Ein wichtiger Grundstein für den wirtschaftlichen Erfolg in der Schweiz ist die Wirtschaftsfreiheit. Unnötige, neue Einschränkungen - in welchem Bereich auch immer - sind zu vermeiden. Der bestehende Datenschutz hat sich bewährt. Die Wirtschaft sieht sich einer starken, mündigen Abnehmer- und Konsumentenschaft gegenüber, die ihren Ansprüchen schon jetzt durchaus Gehör zu verschaffen weiss. Zusätzliche Kontrollgremien sind nach Ansicht des sgv nicht nötig.

4.2 Champ d'application et définitions

Der sgv ist der Auffassung, dass sich die heute dualistische Verantwortung von Bund und Kantonen in der Datenschutzgesetzgebung bewährt hat. Eine Mehrheit der Begleitgruppe schlägt das Auswirkungsprinzip vor. Das Datenschutzrecht würde damit auch Anwendung auf Sachverhalte finden, die sich im Ausland zutragen, aber die in einem wesentlichen Rahmen Auswirkungen auf die Schweiz haben. Der sgv lehnt diese Position ab und unterstützt das Territorialitätsprinzip, da sich doch zu einem wesentlichen Zusatzaufwand bei international tätigen Firmen führen könnten. Zudem ist die Durchsetzbarkeit in der Praxis fraglich.

4.3 Principes généraux de protection des données personelles

Im Normkonzept wird die Stärkung der Informationspflicht des Datenbearbeiters gefordert. Bereits heute gibt es das Auskunftsrecht. Dieses wird – wie im Bericht festgestellt – eher zurückhaltend genutzt. Eine generelle Informationspflicht für jegliches Bearbeiten von Daten ist unverhältnismässig.

Das dem Obligationenrecht zugrundeliegende Zug-um-Zug Geschäft (Ware gegen Barzahlung) wird tendenziell an Bedeutung verlieren. Kann die Bezahlung nicht mehr Zug um Zug abgewickelt werden, so übernimmt notwendigerweise eine der involvierten Parteien das Risiko der Vorleistung und damit das Risiko eines Zahlungsausfalls. Zu den involvierten Parteien können nicht nur der Lieferant gehören, sondern auch aussenstehende Finanzierer (Leasinggeber, Kreditkartenunternehmen). Für den gewerblichen Alltag ist der einfache Zugang zu gesicherten Daten (z.B. zu Bonitätsprüfungen) deshalb von zentraler Bedeutung. Zahlreiche Lieferanten, welche täglich Waren gegen Rechnung liefern, erleiden in der Schweiz Jahr für Jahr hohe Verluste. Schon allein die amtlich erfassten, jährlichen Forderungsausfälle belaufen sich auf Milliarden. Die Betreibungs- und Konkursstatistik des BFS weist für die Zeit zwischen 2008 und 2013 Konkursverluste von mehr als 2 Mia pro Jahr aus. Zahlenmässig werden nur Ausfälle aus den durchgeführten Konkursverfahren erfasst. Weitaus grössere Verluste resultieren aus den mangels Aktiven eingestellten Konkursen (ca. 50 % aller Verfahren) sowie aus zehntausenden von Pfändungsverlustscheinen, die gegen Private und nicht im Handelsregister eingetragene Kleinunternehmen oder wegen unbeglichener Steuerforderungen ausgestellt werden. Laut der offiziellen Statistik mussten 2013 knapp 2.8 Mio. Zahlungsbefehle ausgestellt und mehr als 1,45 Mio. Pfändungen vollzogen werden. Nach Branchenschätzung bescheren Insolvenzen und fruchtlose Pfändungen Wirtschaft und Fiskus Jahr für Jahr Verluste von gegen CHF 11 Mia.

Informationspflichten, die grundsätzlich jedes Personendatum bis hin zur Adresse umfassen, haben übermässig aufwändige Rapport- und Dokumentationspflichten zur Folge und sind im gewerblichen Alltag nicht praktizierbar. Neue Rechtsunsicherheiten und Regulierungen mit hohen Folgekosten werden geschaffen. Unabhängig, ob es sich um eine gesetzliche Vorgabe oder um „good practice" handelt, die aktive Informationspflicht über jegliches bearbeitetes Personendatum wäre mit einem enormen administrativen Aufwand für jeden Inhaber einer Datei verbunden. Oftmals wird sich zudem kaum abschätzen lassen, ob die betroffene Person davon nun Kenntnis hat oder es zumindest wissen müsste, oder eben nicht. Die Rechtsunsicherheit wäre gewaltig. Informationspflicht kann aus Sicht des sgv aus den dargelegten Gründen nicht Bearbeitungsgrundsatz sein.

Dass die Bonitätsauskunft nicht allein auf das Betreibungsregister abstützten kann, zeigt das Beispiel eines Bauherren, der den Generalunternehmer oder die anderen am Bau beteiligten Personen prüfen

will, um sicherzustellen, dass Garantieleistungen auch in der Zukunft erbracht werden können. Eine Garantieverpflichtung nützt nichts, wenn ein Anbieter bereits vor dem Konkurs steht und nur darum ein günstiges Angebot abgegeben hat. In einem solchen Fall reicht die Betreibungsauskunft schon deswegen nicht, weil viele Forderungen aus Kostengründen schon vor der Betreibung abgeschrieben werden. Diese Ausfälle müssen dann von den ehrlichen und pflichtbewussten Konsumenten übernommen werden. Dies widerspricht der geltenden Auffassung, dass derjenige, der einen Schaden verursacht, diesen auch tragen soll. Betreibungsinformationen fallen erst zu einem späten Zeitpunkt an. Es ist für jede Vertragspartei wichtig, frühzeitig zu erfahren, ob die Gegenpartei Zahlungsprobleme hat oder nicht. In Anbetracht der sich gegenüberstehenden Interessen ist es fehl am Platz, Zahlungsinformationen und damit verbundene Angaben der Bearbeitung durch die willkürliche Unterstellung unter den Begriff des Persönlichkeitsprofils der Bearbeitung ganz oder teilweise entziehen zu wollen. Überdies hat ein Anbieter sicherzustellen, dass sich eine Person nicht unnötig überschuldet. Dies kann er nur sicherstellen, wenn er Zugang zu entsprechenden Bonitätsinformationen hat.

Pflicht zur Ernennung eines Datenschutzbeauftragten

Der Verwaltungsrat trägt die oberste Verantwortung und muss die Organisation der Unternehmung nach den Risiken des Unternehmens ausrichten. Im Übrigen auferlegt OR 716a dem Verwaltungsrat die unübertragbaren und unentziehbaren Verpflichtungen. Er hat die Pflicht zur Oberleitung der AG und haftet, wenn er diese Pflicht missachtet. Hierfür führt er eine Risikobeurteilung bzw. ein IKS. Die Pflicht zur Einsetzung eines Datenschutzbeauftragten macht in diesem Zusammenhang keinen Sinn und schiesst über das Ziel hinaus. Mit dem gleichen Recht könnte von jedem Unternehmen ein Produktionsverantwortlicher gefordert werden.

Das heutige DSG ermöglicht Zertifizierungsverfahren und die freiwillige Ernennung eines Datenschutzbeauftragten oder einer Datenschutzbeauftragen in einer Firma. Jede Firma, die überdies mit sensiblen Personendaten operiert, hat ein ureigenes Interesse daran, keine Reputationsschäden zu riskieren.

Der sgv lehnt eine generelle gesetzliche Pflicht zur Ernennung eines Datenschutzbeauftragten für Unternehmen ab, nicht aber für die öffentliche Hand.

Von einer aktiven Meldepflicht von Datenschutzverletzungen ist mindestens im Einzelfall abzusehen. Eine Meldepflicht macht dann allenfalls Sinn, wenn eine sehr grosse Öffentlichkeit, z.B. Tausende von Personen betroffen sind und die Umstände eine Meldung erst rechtfertigen (z.B. verschickt eine Bank an Tausende von Kundinnen und Kunden falsche Kontoauszüge).

4.4 Rechte der betroffenen Personen – Katalog der Rechtsansprüche

Auskunftsrecht: Der wichtigste Grundsatz für eine funktionierende Wirtschaft und ein vertrauensvolles Zusammenarbeiten ist eine objektive Abwägung der sich gegenüberstehenden Interessen. Nicht nur Lieferanten sind an der Möglichkeit von Bonitätsprüfungen interessiert. Auch Konsumentinnen und Konsumenten möchten prüfen, ob sie eine Vorauszahlung an einen Lieferanten leisten sollen oder nicht.

Recht auf Berichtigung: Die Möglichkeit, die Empfänger von Personendaten in Erfahrung zu bringen, widerspricht dem Recht des Datenbearbeiters auf Schutz seiner Kunden. Die Korrekturen haben ohne weitere Angaben über die Informationsempfänger zu erfolgen.

Recht auf Löschung: Zu unterscheiden ist zwischen dem Recht auf „Löschung“ und dem Recht auf „Sperrung“. Für die Sperrung braucht es eine Personenidentifikationsnummer die referenziert werden kann. Bei der Löschung sind in jedem Fall die Daten weg und es kann nicht sichergestellt werden, dass diese in der Zukunft nicht wieder aufgenommen werden. Der Kunde muss sich aber der Folgen bewusst sein. Zudem dürfen nur in begründeten Fällen Daten gelöscht werden, die nicht aus hoheitlichen Quellen stammen. Daten, die von der öffentlichen Hand publiziert werden, sollten nicht gelöscht

werden können. Das Recht auf Löschung darf nicht missbraucht werden um Gutgläubige zu täuschen.

Automatisierte Entscheidungsfindung: Es gibt keinen Anspruch auf Kredit. Insofern muss auch kein „erhöhtes Schutzbedürfnis“ bestehen. Es gibt auch keine Regeln oder Bestimmungen, welche Grundlagen in die Entscheidungsfindung für einen Lieferantenkredit oder Kredit miteinfliessen. Jede Person ist frei in der Auswahl ihrer Kriterien. Die Bonität ist auch nur eines davon. So zählt am Schluss oftmals das Bauchgefühl. Bei der Bearbeitung von einer kleinen Anzahl von Geschäften kann dies individuell gemacht werden und wird von den Unternehmen vielfach in einer „Creditpolicy“ zusammengefasst. Dies ist nötig, damit die Mitarbeitenden wissen wie sie vorzugehen haben. In diesem Fall gibt es für den Betroffenen kein Recht zu erfahren, warum ihm kein Lieferantenkredit gewährt wird. Er kann die Ware ja in jedem Fall kaufen, nur eben nicht auf Kredit sondern gegen Vorauskasse.

Der Vorschlag einer Mehrheit der Begleitgruppe zielt darauf ab, „jeder Person das Recht einzuräumen, keiner auf einer rein automatisierten Bearbeitung von Daten basierenden Entscheidung unterworfen zu werden. Bei einer automatisierten Kreditentscheidung ist das Vorgehen gleich wie im Einzelfall, mit dem Unterschied, dass die Kriterien aufgrund der grossen Anzahl von Transaktionen systemgestützt aufbereitet werden. Subjektive gestützte Beurteilungen werden hingegen eliminiert, was ein Vorteil ist. Das Nichtzulassen automatisierter Einzelentscheidungen ist allerdings ein Eingriff in die Wirtschaftsfreiheit.

Die Abbildung von zahlungsrelevanten Informationen stellt kein Persönlichkeitsprofil dar. Bezahlt jemand eine Rechnungen nicht, oder ist er im Konkursverfahren, so hat der zukünftige Gläubiger das Recht, vor der Gewährung eines Lieferantenkredits zu prüfen, ob bereits Anzeichen auf Zahlungsschwierigkeiten bestehen.

4.8 Besondere Bestimmungen betreffend das Bearbeiten von Personendaten durch private Personen

Beweislastumkehr: Nach den allgemein geltenden Regeln der Beweislastverteilung muss heute die betroffene Person den Nachweis einer Persönlichkeitsverletzung erbringen. Eine Mehrheit der Begleitgruppe möchte die Beweislast umkehren und das Gericht ermächtigen, vom Datenbearbeiter im Einzelfall den Nachweis einer datenschutzkonformen Bearbeitung verlangen zu können. Der sgv lehnt eine solche Beweislastumkehrung ab. Die vorgeschlagene Beweislastumkehr wird im Ergebnis dazu führen, dass Datenbearbeiter alle möglichen Interna offenlegen müssen, um sich gegen die unsubstanzierte Behauptungen zu verteidigen, sie hätten sich nicht datenschutzkonform verhalten. Die Beweislastumkehr läuft auf eine Verschuldensvermutung hinaus und wird vom sgv abgelehnt. Ebenso unterstützt der sgv eine Kausalhaftung zu Lasten des privaten Datenverarbeiters nicht.

Der Vorschlag, die Bearbeitung von Daten juristischer Personen im Rahmen ihres Geschäftszwecks als Rechtfertigungsgrund aufzunehmen, ist zu unterstützen. Nur müsste dieser Rechtfertigungsgrund auf alle Unternehmen ausgedehnt werden, also auch auf Einzelfirmen und Personengesellschaften. Damit ist auch die haftende Person miteinbezogen. Die Anbieterseite ist als Ganzes gleich zu behandeln, zumal sie selbst wählen kann in welcher Rechtsform sie am Markt auftreten will.

Massnahmen zur verbesserten Durchsetzung individueller Ansprüche

Kostenerleichterungen: Mit der Einführung der neuen Prozessordnungen auf 1.1.2011 sind in den Kantonen Kostenvorschüsse für Kläger vor Gerichten eingeführt bzw. massiv erhöht worden. Damit ist die Hürde vor allem auch für gewerbliche Kreise, vor Gericht Recht zu erhalten, erhöht worden. In gewissen Kantonen und Gerichten bewirken hohe Gebühren faktisch eine Zugangsbarriere. Vor diesem Hintergrund ist es schwer vorstellbar, für den partikulären Fall von Datenschutzverletzungen „erheblich reduzierte“ Gerichtskosten festzulegen. Dass die reduzierten Kosten nur für natürliche, nicht aber für juristische Personen gelten sollen, ist ebenfalls schwer nachvollziehbar. Auch juristi-

sche Personen im kleingewerblichen Bereich verfügen nicht über finanzielle Mittel auf Vorrat.

Sammelklagen: Der sgv hat gegenüber Sammelklagen im Bereich des Datenschutzes grosse Vorbehalte.

4.10 Autorités de contrôle

Vorgeschlagen wird, der eidgenössischen Datenschutzbehörde ein Untersuchungsrecht, vergleichbar mit demjenigen der Wettbewerbsbehörde nach Art. 26 KartG zu geben. Nach einer informellen Voruntersuchung hätte die Datenschutzbehörde die Möglichkeit, eine formelle Untersuchung zu eröffnen und auch Bussen zu verteilen. Sie würde damit eine Verfügungsbefugnis erhalten.

Der sgv vertritt die Auffassung, dass die heutigen Möglichkeiten gemäss Art. 29 DSG genügen, wonach der Datenschutzbeauftragte von sich aus oder auf Meldung Dritter einen Sachverhalt im Privatrechtsbereich abklärt, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler); Datensammlungen registriert werden müssen (Art. 11*a*) oder eine Informationspflicht nach Artikel 6 Absatz 3 DSG besteht. Der Datenschutzbeauftragte kann entsprechende Empfehlungen erlassen. Aus Sicht des sgv sind zusätzliche Gremien nicht nötig.

Finanzierung des Datenschutzes: Der Schweizerische Gewerbeverband sgv unterstützt die bisherige Alimentierung des Datenschutzbeauftragten und seiner Mitarbeitenden aus dem Bundeshaushalt. Zusätzliche Finanzierungsmittel wie z.B. eine Abgabepflicht für Betriebe lehnt der sgv ab. Auch eine Finanzierung aus Bussen ist für den sgv nicht zielführend.

Schlussbemerkungen

Die Diskussion um den Datenschutz vor dem Hintergrund neuer Technologien und Entwicklungen ist wichtig. Datenschutz darf nicht nur aus der Optik von „Social media“, „Google“, usw. betrachtet werden. Aufgrund der hohen Nutzerzahl der sozialen Medien haben sich die Datenschutzbedürfnisse stark verändert. Das „Recht auf Vergessen“ wird stipuliert und ohne weiteres auf alle Datenverarbeiter und jede Form der Datenbearbeitung ausgedehnt. Den Auswirkungen auf Gewerbe und Wirtschaft muss dabei viel mehr Beachtung geschenkt werden. Datenschutz darf nicht dazu führen, dass Schuldner ein Recht auf die Löschung ihres negativen Zahlungsverhaltens erhalten. Die kürzlich erschienene Studie von Deloitte „Economic impact assessment of the proposed European General Data Protection Regulation“ zeigt unter anderem auf, was die wirtschaftlichen Auswirkungen sind und was für Bereiche von der Novellierung der Datenschutzgrundverordnung betroffen sind.[1]

Ebenfalls mit in die Überlegungen einzubeziehen sind:

- **Direct Marketing** als grundlegende Quelle der Kommunikation zwischen den Anbietern und deren Kunden. Die Möglichkeit, bestimmte Gruppen von Kunden zielgerichtet anzusprechen, ist das Schlüsselkriterium für die Abgrenzung von anderen Formen des Marketings.
- **Online Behavioural Advertising** bezieht sich auf die Verwendung von Online-Daten um die Interessen von Usern mit den spezifischen Angeboten abzustimmen.
- **Web Analytics** hilft Anbietern dem Konsumenten mit einer besseren Qualität und relevanteren Inhalten zu versorgen.
- **Credit Information**: Bonitätsinformationen sind wichtige „Enabler“ der Wirtschaft und versorgen die sie mit den notwendigen Tools, um das Ausfallrisiko zu bestimmen. Dies hilft die Kosten für die Güter zu verringern und vereinfacht den Onlinebezug von Gütern.

---

[1] Deloitte, Economic impact assessment of the proposed European General Data Protection Regulation, 2013; Seite 6 ff.

Diese vier Bereiche sind von erheblicher wirtschaftlicher Bedeutung und müssen in die Erwägungen miteinbezogen werden. Insgesamt ist sicherzustellen, dass nicht auf Kosten der Wirtschaft vermeintlich konsumentenfreundliche Regulierungen erfolgen, die anschliessend auf die Konsumenten zurückfallen.

Dieter Kläy

Ressortleiter

Bemerkungen Normenkonzept Revision DSG

VUD | David Rosenthal, 30. September 2014

Die folgenden Kommentare beziehen sich auf das Normenkonzept und Kommentare anderer Mitglieder der Begleitgruppe. Sie stützen sich auf Inputs aus dem VUD und meine persönlichen Erfahrungen.

A. Einleitende Bemerkungen

Der Bundesrat hat dem BJ den Auftrag erteilt, eine Revision des DSG zu prüfen. Wir sind jedoch nach wie vor der Ansicht, dass in der Sache kein Bedarf an einer Revision steht. Zwar ist der Datenschutz in den Schlagzeilen wie nie zuvor, doch das hat nur damit zu tun, dass er heute verstärkt Beachtung findet und durchgesetzt wird, nicht, dass er nicht hinreichend ist.

Sämtliche Fälle, die in der Schweiz zu einer gerichtlichen Beurteilung führten oder in denen die Behörden aktiv geworden sind, haben bewiesen, dass die gesetzlichen Grundlagen genügen. Sie haben sogar aufgezeigt, dass der Datenschutz heute tendenziell zu weit geht.

Als Beispiel sei ein ganz aktueller Fall erwähnt, in welchem ein Schweizer Gericht unter dem Titel des Datenschutzes selbst die Bearbeitung von *anonymen* Daten verboten hat, und das DSG anwandte, obwohl unbestrittenermassen gar keine Personendaten vorlagen.

Das Beispiel zeigt – wie etliche andere Prozesse im Bereich des Datenschutzrechts auch – dass die betroffenen Personen keineswegs am kürzeren Hebel sind. DSG ist technologieneutral und die darin enthaltenen Grundsätze sind nach wie vor richtig. Dass der Datenschutz mit den aktuellen technologischen Entwicklungen nicht Schritt halten kann, ist zwar eine weitverbreitete, politisch attraktive Behauptung, aber letztlich durch nichts belegt.

Richtig ist, dass die Fälle, in denen die Regeln verletzt wurden oder in denen die zur Anwendung dieser Regeln nötigen Wertungen diskutiert werden, sehr viel medienträchtiger sind und mehr Personen betreffen und vor allem internationaler sind als in der Vergangenheit. Die Regeln deswegen als ineffektiv oder gar überholt zu bezeichnen, ist ein Trugschluss.

Auch die in den Arbeiten immer wieder gehörte Aussage, niemand ausser einigen Experten würden das DSG verstehen, ist aus unserer Sicht falsch. Abstrakte Regeln gehören zum Wesen des schweizerischen Rechts und sind gerade einer der Gründe, warum das DSG auch heute noch funktioniert. Wird kritisiert, dass der Normalbürger bei der Lektüre des DSG nicht wisse, was er zu tun habe, so gilt dasselbe für das ZGB und OR. Kein "Normalbürger" kennt sich heute noch z.B. mit den Regeln im Kündigungsschutz im Arbeitsbereich oder Mietrecht aus; der Blick ins Gesetz genügt schon lange nicht mehr. Man muss Experte im Arbeits- oder Mietrecht sein, um zu verstehen, was wirklich gilt.

Das ist aber kein Fehler des Rechts, sondern zeigt die Entwicklungsfähigkeit abstrakter Regeln und es belegt die Komplexität unserer Welt. Die Dinge sind eben nicht so simpel, und wer

glaubt, dies auf einfache Weise mit neuen Regeln zu lösen, schadet der Sache. Es wäre schade, wenn wir die Schweizer Rechtstradition durch die heute leider weit verbreiteten populistischen und sehr eingängigen, aber zu kurz gedachten Forderungen im Bereich des Datenschutzes über Bord zu werfen.

Übrigens ist auch das heutige Instrument von Art. 29 DSG, dass dem EDÖB ein umfassendes Klagerecht gibt, vollauf genügend und sehr effizient ist. Es ist klar, dass dies eine politisch nicht opportune Aussage ist, da alles nach "Stärkung" des Datenschutzes schreit und ein EDÖB, der lediglich "Empfehlungen" aussprechen statt verfügen kann, als zahnlos erscheinen mag (auch wenn dies in der Praxis seinem Klagerecht in keiner Weise gerecht wird; er kann heute faktisch genauso Druck ausüben wie wenn er selbst Anordnungen treffen könnte, wie zahlreiche Beispiele zeigen). Dass der EDÖB selbst Verfügungskompetenz möchte, ist vor diesem Hintergrund zwar nachvollziehbar, aber nicht zielführend und notwendig.

Aber bei Lichte betrachtet ist das einzige Problem, das der Durchsetzung des DSG durch den EDÖB im Wege steht, der Mangel an Ressourcen des EDÖB. Dieses Problem werden die vorgeschlagenen Anpassungen nicht lindern, sondern verschärfen. Sie mögen politisch unvermeidlich sein, aber die Schweiz wird dem Datenschutz (und der Wirtschaft, die die Kosten zu tragen hat) damit keinen Gefallen erweisen; die Anwälte und Berater werden sich hingegen freuen. Sie haben es schon im Bereich des Kartellrechts getan, aber die Kosten der Datenschutzaufsicht werden explodieren oder, falls die Ressourcen nicht zur Verfügung gestellt werden, in den eigenen Verfahrensbestimmungen stecken bleiben.

Es ist klar, dass die Schweiz im Falle einer Verabschiedung der revidierten Europaratskonvention 108 deren Regelungen irgendwie übernehmen muss. Sie sollte dabei jedoch nicht einfach etwas weltfremde Regelungen (wie z.B. bei den automatisierten Einzelfallentscheidungen oder der Transparenz, welche zu einer Inflation an "Hinweisen" führen wird, die am Ende nicht mehr Transparenz verschaffen werden, als es die kleingedruckten Geschäftsbedingungen von iTunes schon tun) mit dem Argument übernehmen, man müsse das eben tun. Die Schweiz hat in solchen Fällen einen erheblichen Spielraum bei der Umsetzung und sollte ihn mit Augenmass nutzen, auch wenn zu wünschen gewesen wäre, dass die Revision der Konvention von einem etwas ausgeglichenerem Gremium ausgearbeitet worden wäre.

B. Einige konkrete Bemerkungen

1. Best Practice

Die Best Practice-Regeln werden nur dann ihren Zweck erfüllen, wenn sie den Datenbearbeitern Rechtssicherheit geben. Der VUD regt an, ausdrücklich auf die Regelung in Österreich zu verweisen, wo es "genehmigte" Good-Practice-Regelungen schon gibt. Hier findet sich ein Beispiel:

https://www.wko.at/Content.Node/branchen/sbg/BankVersicherung/Banken-und-Bankiers/Verhaltensregeln-fuer-Gluecksspielbetreiber-1.html

2. Begriffsdefinitionen

Es ist nicht sinnvoll, Begriffe wie das "Territorialitätsprinzip", die durch die Rechtssprechung vor dem Hintergrund der laufenden gesellschaftlichen Entwicklung ständig weiterentwickelt werden, festzuschreiben und damit einer Weiterentwicklung zu entziehen. Damit wird genau jener Fehler begangen, von dem man glaubt, ihn mit der jetzigen Revision beheben zu müssen, nämlich dass das DSG von der technologischen und gesellschaftlichen Entwicklung überholt wird. Dies ist nicht der Fall, doch gewisse der ins Auge gefassten Anpassungen werden das DSG so sehr auf ganz bestimmte Praxisanwendungen konkretisieren, dass das DSG nicht mehr "passen" wird, wenn sich die Fragestellungen, Wertvorstellungen oder andere Aspekte auch schon nur leicht ändern. Das DSG ist zwar schon viele Jahre alt, aber der Umstand, dass es so allgemeingültig formuliert ist, macht es auch sehr flexibel. Der Fall Google Street View hat bewiesen, dass sich das DSG bestens auch im Zeitalter der internationalen Internetdienste anwenden lässt.

Beim Umgang mit Personendaten sind grundsätzlich folgende Funktionen zu unterscheiden: (A) die natürliche oder juristische Person, welche für die Bearbeitung von Daten in irgend einer Form zuständig und verantwortlich ist: “controller“ im Sinne von Art. 2.d RL 95/46/EG; (B) der “Inhaber einer Datensammlung“ im Sinne von Art. 3 Bst. i DSG; (C) der “Auftragsdatenbearbeiter“ (“processor“ im Sinne von Art. 2.e RL 95/46/EG), d.h. jener Dritte im Sinne von Art. 10a DSG, welcher Daten im Auftrag eines Auftraggebers bearbeitet. Bisher fehlt im schweizerischen Datenschutzrecht eine Definition welche in Abgrenzung zum “Inhaber der Datensammlung“ nach Art. 3 Bst. i DSG und Art. 2 d) der Europaratskonvention ETS Nr. 108 “controller of the file“ die für eine Bearbeitung von Personendaten verantwortliche Person oder Stelle definiert. Wir betrachten die beiden Begriffe “Inhaber der Datensammlung“ sowie “bearbeitende Stelle“ keineswegs als gleichwertig, wie u.E. zu Unrecht im Normkonzept angenommen wird, sondern als auf erheblich verschiedene Tatbestände bezogene Begriffe bzw. Funktionen. Auch wenn im europäischen Ausland die verschiedenen Begriffe zum Teil durchmischt werden, erachten wir es als sinnvoll, hier weiterhin klar zwischen den verschiedenen Funktionen zu trennen.

Nach geltendem schweizerischen Recht werden die “Persönlichkeitsprofile“ gemäss Art. 3 Bst. d DSG durchgehend den gleichen Anforderungen unterstellt wie die “besonders schützenswerten Personendaten“ nach Art. 3 Bst. c DSG. Nun soll die für das schweizerische Datenschutzrecht von 1992 originelle und weit in die Zukunft greifende Definition des “Persönlichkeitsprofils“ gestrichen und durch spezielle Regelungen zum “Profiling“ ersetzt werden. Es stellte sich bei uns bei nochmaliger Betrachtung die Frage, wieviel damit gewonnen würde. Denn auch bei den Bestimmungen über das “Profiling“ wird man um eine entsprechende, wegen der Tragweite der Bestimmung heikle Definition der “Persönlichkeitsprofile“ nicht herumkommen.

3. Informationspflicht

Es ist sinnvoll, die heute in Art. 14 und 18a/b DSG zusätzlich vorgesehene Informationspflicht zugunsten eines allgemeinen Grundsatzes der Transparenz aufzuheben. Es muss jedoch darauf geachtet werden, dass die selbständige Informationspflicht nicht zu einem übermässigen bürokratischen Aufwand führt wie bei den heute in der Praxis kaum sinnvoll umsetzbaren Art.

14 und 18-18b DSG. Eine Pflicht zur Information der betroffenen Personen über jede der heute allgegenwärtigen, aber auch alltäglichen Datenerfassungen und -bearbeitungen bei jeder Art elektronischer Kommunikation geht schlicht zu weit, Europarat hin oder her. Hier ist im Normenkonzept nochmals zu betonen, dass eine vernünftige, sachgerechte und zurückhaltende Umsetzung anzustreben ist, die nicht zu einer Inflation der Information führt, die gar nichts bringt, ja sogar kontraproduktiv ist.

4. Auskunftsrecht

Der Zugang externer Personen zu firmeninternen Unterlagen muss restriktiv gehandhabt werden, schon aus Gründen der Datensicherheit. Es besteht heute schon eine Tendenz der Gerichte, externen Personen durch ausufernde Auskunftsansprüche Zugang zu allen möglichen internen Unterlagen von Unternehmen zu geben, selbst wenn es überhaupt nicht um den Datenschutz geht; das Auskunftsrecht wird immer häufiger missbraucht, um Beweismittel für datenschutzfremde Zwecke zu sammeln, Unternehmen zu schikanieren und auszuforschen. Ein Ausbau der Zugangsrechte, wie teilweise auch hier gefordert, ist nicht angezeigt.

Bezüglich der heutigen Regelung ist es zwingend, dass im Falle eines strittigen Auskunftsgesuchs, die Interessenabwägung immer auch die Interessen des Inhabers der Datensammlung berücksichtigt werden. Es gibt keinen sachlogischen Grund, warum seine Interessen per se nicht beachtlich sind, wenn er die Daten, um die es geht, bereits an Dritte weitergegeben hat (wozu z.B. ein konzerninterner Datenverkehr schon genügen kann). Genau dies sieht Art. 9 Abs. 4 DSG heute aber vor. Der bestehende Zusatz "und er die Personendaten nicht Dritten bekannt gibt" ist in dieser Bestimmung daher ersatzlos zu streichen. Es gibt keinen Grund zur Befürchtung, dass die Gerichte, welche die Interessenabwägung letztendlich vornehmen müssen, dies nicht sachgerecht tun werden. Heute wird ihnen aber in den erwähnten Fällen die Vornahme einer Interessenabwägung untersagt.

Es wurde im Kreise des VUD noch angeregt, beim Auskunftsrecht vorzusehen, dass die betroffene Person dann, wenn sie Auskunft über Sicherungs- und Archivdaten sucht, ein rechtlich geschütztes Interesse glaubhaft zu machen hat; hier also höhere Anforderungen gelten sollen (vgl. dazu § 19(1) und (2) sowie §§ 33(2) Ziff. 2 und 34 (7) BDSG). Das rechtfertigt sich umso mehr, als Unternehmen immer stärker durch den Gesetzgeber zur Aufbewahrung von Daten verpflichtet werden. Als sinnvoll erachtet wird auch, eine Mitwirkungspflicht der betroffenen Person zum Auffinden der Daten zu statuieren.

5. Zustimmung

Die geltende Regelung betreffend Zustimmung soll beibehalten werden. Die im Europarat und in der EU teilweise diskutierten Anpassungen rühren von einem dort – anders als in der Schweiz – praktizierten Verständnis des Begriffs der Einwilligung her. In der Schweiz sind die Anforderungen an eine Einwilligung schon relativ hoch. Der Unterschied z.B. zwischen einer "klaren" und "nicht klaren" Einwilligung ist dem Schweizer Recht wesensfremd; entweder liegt eine Einwilligung vor oder aber eben nicht. Wir möchten zudem ausdrücklich davor warnen, von einer fehlenden Einwilligung auszugehen, wenn eine betroffenen Person sich über die Datenbearbeitung nicht erkundigt, welche die von der bearbeitenden Stellen zugänglich gemachten

Angaben über die Bearbeitung der Daten nicht gelesen oder diese nicht verstanden hat, und unüberlegt das “Gelesen und Verstanden-Häklein“ unter ein Angebot im Web gesetzt hat. Voraussetzung für eine gültige Einwilligung ist natürlich eine “angemessene vorangehende Information“ im Sinne von Art. 4 Abs. 5 DSG. Es kann diesbezüglich auf die Gerichtspraxis zu “ungelesenen oder nicht verstandenen AGB“ unter Vorbehalt der Ungültigkeit von ungewöhnlichen, einseitigen, irreführenden AGB verwiesen werden: Zusammengefasst in BGE 109 II 213. Es gibt auch hier keinen Grund, dies im Datenschutz anders als im ganzen Rest des Schweizer Rechts zu regeln.

6. Widerspruchsrecht

Das Widerspruchsrecht ist nicht auszubauen, weil es heute schon besteht und nicht erwiesen ist, warum es nicht genügen soll. Im Gegenteil: hat das Google-Urteil des EuGH jüngst gerade wieder belegt, wie streng das heutige Datenschutzrecht sein kann, wenn es tatsächlich genutzt wird. Das Urteil zeigt aber auch die Schattenseiten auf (Zensurdiskussion). Das Datenschutzrecht sollte zudem wertungsfrei bleiben und nicht dafür benutzt werden, die Weiterentwicklung unserer Wertordnung aufzuhalten, bloss weil man sie für heikel hält. Die Profilbildung wird in unserer Gesellschaft immer wichtiger, weil es je längers je mehr Möglichkeiten gibt, solche zu bilden; sie hat aber wie alles ihre guten und schlechten Seiten. Profile können etwa auch dazu dienen, Entscheide vorhersehbarer, transparenter zu machen. Und Unternehmen können durch Profile missbräuchliche Verhaltensweisen immer besser erkennen. Die Profilbildung zu verteufeln, ist nicht sachgerecht. Es kann daher nicht Sache des Datenschutzrechts sein, der Profilbildung durch ein spezifisches Widerspruchsrecht pauschal einen Riegel schieben zu wollen.

7. Datenportabilität

Das Recht auf Datenportabilität hat im Datenschutzrecht nichts zu suchen. Es geht dabei nur um die Regulierung der Marktzugangs zu sozialen Netzwerken. Das ist eine typische "Denkzettel"-Regel einiger EU-Politiker und Datenschützer, denen Facebook ein Dorn im Auge ist, deren Auswirkung aber niemand versteht und deren Kosten schon gar nicht. Wir sollten nicht den Fehler machen, solche Dinge in unser Recht zu übernehmen; dies ist überdies ein massiver Eingriff in die Wirtschaftsfreiheit. Falls sich die Datenportabilität auf EU-Ebene tatsächlich durchsetzen sollte, würden die Schweizer Kunden bei solchen Diensten ohnehin automatisch mitprofitieren.

8. Ausländische Gerichts- und Behördenverfahren als Rechtfertigungsgrund für Exporte

Die geforderte Ausdehnung des Rechtfertigungsgrunds bei Datenexporten von Gerichten auf Behörden ist sachgerecht. Ein Unternehmen darf heute Unterlagen liefern, wenn es im Ausland angeklagt worden ist oder selbst gegen jemanden klagt, und sei es wegen einer belanglosen Sache (Art. 6 Abs. 2 Bst. d DSG). Es darf aber keine Unterlagen liefern, wenn dies im Rahmen eines vorgerichtlichen, aber ebenso regulierten Behördenverfahrens erforderlich ist, zum Beispiel die eigene Unschuld zu beweisen. Diese Unterscheidung ist nicht nachvollziehbar. Ein Unternehmen wird heute dadurch gezwungen, entweder das DSG zu verletzen oder bei einer Behördenuntersuchung die Kooperation zu verweigern und es zu einer Anklage vor Gericht – mit potenziell katastrophalen Folgen für alle Beteiligten – kommen zu lassen, da erst dann nach

DSG geliefert werden darf. Das macht keinen Sinn. Die Regelung ist daher auf Behördenverfahren auszudehnen.

9. Zertifizierungspflicht

Die Zertifizierungspflicht im Bereich der Krankenversicherung ist letztlich ein Kompromiss im Streit um die Einführung der Fallpauschalen; sie kann und sollte keineswegs als Vorbild für weitere Zertifizierungspflichten für andere Bereiche dienen. Die Zertifizierungen und damit verbundenen Aufwände kosteten den Prämienzahler bereits Millionen, ohne, dass sie wirklich einen Zusatznutzen bringen. Eine Zertifizierung belegt einzig, dass ein Datenschutzmanagementsystem existiert, also entsprechende Prozesse und Dokumentationen vorhanden sind, es belegt aber in keiner Weise, ob der Datenschutz wirklich eingehalten wird. Datenschutzverstösse verhindert auch ein DSMS nicht. Es gibt einen guten Grund, warum sich Unternehmen nicht für Zertifizierungen nach Art. 11 DSG interessieren. Solange sie freiwillig sind, schaden sie nichts. Wird die Zertifizierungspflicht aber ausgedehnt, dient dies vor allem der Zertifizierungsbranche. Soll in gewissen Branchen der Datenschutz verstärkt werden, sind Kontrollen und Untersuchungen, wie sie bisher praktiziert wurden, wesentlich wirksamer und nachhaltiger.

10. Rechtfertigungsmöglichkeit auch bei Verletzung der Datenschutzgrundsätze

Es wurde angeregt, dass Art. 12 Abs. 2 Bst. a DSG entgegen dem Vorschlag im Normenkonzept so belassen wird, wie er heute im Gesetz ist. Dies ist abzulehnen. Der EDÖB hatte dies im Fall Logistep so vertreten, aber das Bundesgericht hat festgestellt, dass es sich um ein Versehen handelte (wie in der Lehre mit Verweis auf die Sitzungsprotokolle nachgewiesen wurde; das Parlament ging damals von einer falschen Annahme aus). Es hielt fest, dass auch Verletzungen der Bearbeitungsgrundsätze gerechtfertigt werden können. Dies entspricht auch einem Grundprinzip des Persönlichkeitsschutzrechts entspricht. Der Fall, in welchem der Entscheid zustande kam, war jedoch ein sehr schlechter Fall und das Bundesgericht wurde für seine Interessenabwägung zugunsten des Datenschutzes massiv kritisiert. Aus der Not gebar es die Formel, dass eine Rechtfertigung eben nur mit grosser Zurückhaltung zulässig sei. Diese Formel wird inzwischen vom EDÖB und auch den Gerichten gebetsmühlenmässig wiederholt wird. Das Bundesgericht hält sich selbst allerdings nicht (mehr) daran, sondern praktiziert die Interessenabwägung so, wie eine Interessenabwägung überall im Schweizer Recht vorzunehmen ist: Durch schlichtes Abwägen aller auf dem Spiel stehenden Interessen. So gilt es heute auch. Bereits im Fall Google Street View wurde die Interessenabwägung wieder wie vor der letzten Revision durchgeführt. Die Sache sollte im Normenkonzept korrekterweise ausdrücklich beim Namen genannt werden, nämlich dass es sich bei der heutigen Formulierung um ein Versehen handelte. Das gesetzgeberische Versehen sollte definitiv korrigiert werden.

11. Verfügungskompetenz des EDÖB, kollektive Klageinstrumente

Wie eingangs erwähnt ist es wenig sinnvoll, den EDÖB durch Verfügungskompetenzen verfahrensmässig unnötig zu belasten. Er wird mehr Ressourcen benötigen, und die wenigen zusätzlichen Ressourcen, die er erhalten wird, werden für die Wahrung der nötigen Verfahrensvorschriften und -garantien verbraucht werden. Damit ist dem Datenschutz nicht gedient, und inzwischen scheint diese Erkenntnis verschiedenenorts zu reifen.

Wenn nun stattdessen auf Instrumente wie Verbands- oder Sammelklagen ausgewichen werden soll, wird dies den Datenschutz zusätzlich schwächen. Die Datenschutzverbandsklage gibt es seit Jahren und sie ist toter Buchstabe. Die Sammelklage wird in Datenschutzbelangen ebenfalls toter Buchstabe (was die Stärkung des Datenschutzes betrifft) bleiben, birgt aber einiges an Missbrauchspotenzial. Der Datenschutz eignet sich schlicht nicht für Sammelklagen. Und dort, wo es darum geht, gegen eine bestimmte Art der Datenbearbeitung einer bestimmten Person an sich vorzugehen, haben wir bereits das Verfahren nach Art. 29 DSG, das ausgezeichnet funktioniert und erprobt ist. Es ist zugleich das volkswirtschaftlich günstigste Instrument.

Google Street View oder Moneyhouse sind Paradebeispiele, dass das Verfahren nach Art. 29 DSG, in welchem der EDÖB quasi stellvertretend für die betroffenen Personen gegen eine Datenbearbeitung in grundsätzlicher Art und Weise vorgeht, funktioniert und zielführend ist. Kein Verein hätte eine solche Klage gegen Google Street View oder Moneyhouse geführt, eine Sammelklage wäre nie in Frage gekommen. Soll der EDÖB allerdings Verfügungskompetenz erhalten, wird er zwangsläufig wesentlich weniger frei in der Wahl seiner Fälle sein. Auch das ist ein Grund, am bisherigen System festzuhalten.

12. Prozessuale Instrumente

Die Beweislastumkehr läuft, wie entsprechende Kommentatoren festgestellt haben, auf eine Vermutung der "Schuld" hinaus. Hier möchten wir nochmals zu bedenken geben, dass eine Beweislastumkehr in der Praxis unnötig ist. Der Schutz des Einzelnen scheitert in Datenschutzfällen nie am Problem der Beweislast, und es gibt auch keinerlei Belege für solche Fälle. In Tat und Wahrheit sieht das Schweizer Zivilprozessrecht schon heute weitgehende Mitwirkungspflichten seitens einer beklagten Person vor.

Es sei an dieser Stelle – wie schon in der Redaktionsgruppe – betont, dass es keinen Sinn macht, aus reiner Symbolik Dinge, die im Schweizer Zivilprozessrecht ausgiebig, gerecht und sachgerecht geregelt sind, für das Datenschutzrecht nochmals und zudem anders zu regeln. Es gibt keinen Grund, den Datenschutz anders zu behandeln. Auch für eine Kausalhaftung gibt es keinen Anlass. Sie belastet lediglich die Unternehmen, die solche Risiken in ihrer Kalkulation finanziell unterlegen und letztlich auf die Konsumenten überwälzen müssen, ohne, dass ihnen dies jedoch wirklich zu Gute kommt.

Die vorgeschlagenen Kostenerleichterungen braucht es in der Praxis nicht. Sie belasten nur die Staatskasse, werden aber den Rechtsschutz von Privatpersonen nicht stärken. Wenn überhaupt Kosten ein Hinderungsgrund für die Rechtsdurchsetzung sind, dann nicht die Gerichtskosten, sondern die Kosten für die anwaltliche Vertretung und die Pflicht, die gegnerischen Kosten im Falle eines Unterliegens tragen zu müssen.

Wenn aber aus politischen bzw. symbolischen Gründen eine Kostenerleichterung vorgesehen werden sollte, so hat sie für alle Verfahren von Konsumenten zu gelten, die dieselben Themenkomplexe betreffen, so namentlich UWG, DSG und ZGB 28. Andernfalls könnten die betreffenden Ansprüche aus prozessualen Gründen nicht mehr zusammen geltend gemacht werden, wie dies in der Praxis regelmässig geschieht; den betroffenen Personen wäre ein Bärendienst er-

wiesen. Im Grunde sollte es also gar keine Kostenerleichterung geben, und wenn doch, dann höchstens eine, die einer Klagehäufung nicht im Wege steht.

Der Hinweis, dass der Rechtfertigungsgrund von Daten juristischer Personen im Rahmen ihres Geschäftszwecks bzw. ihrer Geschäftstätigkeit auch auf Personengesellschaften und Einzelfirmen auszuweiten ist, erscheint an sich berechtigt; allerdings muss dies einhergehen mit der Definition des Begriffs der Personendaten (d.h. wenn im Rechtfertigungsgrund auch Einzelfirmen berücksichtigt werden, dann sollte auch der Begriff des Personendatums Daten von Einzelfirmen umfassen, was nicht der Fall ist, da sich sonst das Problem gar nicht stellt, weil deren Daten nicht vom DSG erfasst sind).

C. Abschliessende Bemerkung

Die Bemerkungen sind aufgrund sprachlicher Hindernisse (französische Teile des Normenkonzepts) nicht als abschliessende Stellungnahme bzw. Zustimmung zu allen anderen Teilen des Normenkonzepts zu verstehen.