

# Révision de la loi fédérale sur la protection des données : mettre l'accent sur la transparence et le contrôle

La technologie et la réglementation au plan européen évoluent. La législation suisse doit s'adapter. *Camille Dubois*

**Abrégé** La loi fédérale sur la protection des données (LPD) date de 1992. La technologie ayant progressé rapidement, l'Office fédéral de la justice (OFJ) a décidé en 2008 de faire évaluer la loi, afin de savoir si elle offrait toujours une protection suffisante. Il ressort de cette évaluation ainsi que des travaux du Département fédéral de justice et police (DJFP) qui ont suivi que ce n'est, dans certaines situations, pas le cas. Le Conseil fédéral a, dès lors, chargé le DJFP d'élaborer un projet de révision. Celui-ci devrait notamment permettre à la Suisse de ratifier la nouvelle convention STE 108 du Conseil de l'Europe et de transposer les prochaines dispositions de l'UE en la matière, dans la mesure où elles relèvent de l'acquis de Schengen/Dublin. Il est, entre autres, envisagé d'améliorer la transparence des traitements de données ainsi que la maîtrise et le contrôle de ces dernières, de renforcer les pouvoirs du Préposé fédéral à la protection des données et à la transparence (PF PDT) et de promouvoir les bonnes pratiques et l'autorégulation. Le projet destiné à la consultation externe doit être soumis au Conseil fédéral fin août 2016 au plus tard.

La loi fédérale sur la protection des données (LPD; RS 235.1) a été adoptée par le Parlement le 19 juin 1992. Il s'agissait alors de faire face à l'augmentation des risques d'atteinte à la personnalité que comportaient l'utilisation des technologies modernes de l'information et de la communication ainsi que l'intensification massive des traitements de données. Or, à l'époque, le paysage en matière de protection des données était très différent de celui d'aujourd'hui. On ne parlait pas encore d'Internet pour tous et l'accès à l'informatique ne s'était pas encore démocratisé. Aujourd'hui, tout le monde dispose d'un ordinateur, d'un téléphone portable ou d'une tablette connectés; il est question d'Internet des objets, de géolocalisation, de mégadonnées (« big data »), de réseaux sociaux ou encore d'informatique en nuage (« cloud computing »).

## Adapter la loi à l'évolution technologique et au droit européen

Compte tenu de ces développements technologiques et du grand nombre de personnes concernées par la protection des données, l'Office fédé-

ral de la justice (OFJ) a décidé en 2008 de faire évaluer la LPD, conformément à l'article 170 de la Constitution fédérale. Le but était de mesurer l'efficacité de la loi<sup>1</sup>. En raison du champ d'application très vaste de la LPD et des ressources limitées, l'évaluation s'est concentrée sur certains aspects de la loi, à savoir sa notoriété et les mécanismes de mise en œuvre. Il en résulte que le niveau de protection est bon dans les domaines où les défis étaient déjà connus lorsque le texte est entré en vigueur. Les développements technologiques et sociétaux intervenus depuis lors représentent, toutefois, autant de nouvelles menaces pour la protection des données que la loi ne peut plus palier dans certains contextes<sup>2</sup>.

Sur la base de ce constat, le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP), dont dépend l'OFJ, d'examiner les mesures législatives qui permettraient de combler ces lacunes. Le DFJP, dans son examen, devait notamment tenir compte des réformes en cours au niveau de l'UE, qui planche sur un projet de règlement<sup>3</sup> ainsi que de directive<sup>4</sup>, et du Conseil de l'Europe qui procède à une modernisation de sa Convention STE 108<sup>5</sup>. Le contenu de ces textes est important pour la Suisse. Le projet de directive fait en effet partie du développement de l'acquis Schengen et devra être transposé par la Suisse pour les traitements s'inscrivant dans le cadre de la coopération policière et judiciaire qui découle des accords conclus. Quant au projet de règlement, l'UE pourrait le considérer comme faisant partie du développement de l'acquis Dublin et donc y lier la Suisse. Même si l'on fait abstraction de ces considérations, la Suisse aurait tout intérêt à s'inspirer de la législation européenne si elle souhaite continuer de bénéficier d'une décision d'adéquation<sup>6</sup>. Ces réformes devraient aboutir d'ici 2016.

<sup>1</sup> Certaines dispositions, soit celles introduites au 1<sup>er</sup> janvier 2008 (RO 2007 4983) et au 1<sup>er</sup> décembre 2010 (RO 2010 3387), ont expressément été exclues du champ d'application de l'évaluation, en raison de l'absence de recul quant à leurs effets.

<sup>2</sup> *Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht*, 10 mars 2011, pp. 172 et 213s.; disponible en ligne sur le site de l'OFJ (*Rapport du Conseil fédéral du 9 décembre 2011 sur l'évaluation de la loi fédérale sur la protection des données* (FF 2012 255).





KEYSTONE

## Le projet est sur les rails

Au printemps dernier, suite au rapport<sup>7</sup> du groupe chargé d'accompagner les travaux, le Conseil fédéral a confié au DJFP le soin d'élaborer un projet de révision d'ici fin août 2016. Celui-ci devrait notamment permettre à la Suisse de ratifier la nouvelle Convention STE 108 du Conseil de l'Europe, ainsi que de transposer la nouvelle directive et le nouveau règlement de l'UE dans la mesure où ils relèvent de l'acquis de Schengen/Dublin. La révision devrait aussi mettre en œuvre la recommandation émise par les experts européens dans le cadre de l'évaluation Schengen 2014 de doter le Préposé fédéral à la protection des données et à la transparence (PFPDT). Le projet pourrait contenir des mesures qui tendront à :

1. *Promouvoir les bonnes pratiques et l'autorégulation.* Il s'agirait notamment de confier à un organe (par exemple un comité d'experts) le soin d'édicter ou d'approuver des règles de bonnes pratiques. Celles-ci pourraient aussi être élaborées par la branche. Sans être

contraignantes, ces règles serviraient de référence pour les responsables du traitement. Elles permettraient, entre autres, de trouver des solutions adaptées aux nouveaux développements technologiques sans réglementer de manière excessive. Les responsables du traitement disposeraient d'une certaine latitude dans le choix des solutions, lesquelles pourraient être modulées selon les risques, le volume ou le type de données traitées.

2. *Prendre en compte les exigences de protection des données dès la conception et par défaut* (principe de la «privacy by design» et de la «privacy by default»). Il s'agirait, par exemple, d'introduire une obligation pour le responsable du traitement de procéder à une analyse d'impact en cas de risque accru pour la personnalité. Celui-là devrait mettre en place des mesures appropriées notamment en fonction des risques encourus, de l'état de la technique et des coûts. Par ailleurs, il devrait privilégier les réglages par défaut qui sont les plus favorables à la protection des données. Une autre mesure

Le mandat de la Confédération en matière de protection des données devrait aboutir à une révision qui élargirait les compétences de la loi. le préposé Hanspeter Thür s'exprime devant des journalistes.

<sup>3</sup> Projet de règlement relatif à la protection des données des personnes physiques à l'égard du traitement des données à caractère personnel. Il est destiné à remplacer l'actuelle 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).



serait de donner la possibilité au responsable de traitement d'avertir le PFPDT, afin de s'assurer qu'il n'existe pas d'obstacle au traitement envisagé et d'éviter d'éventuelles sanctions.

3. *Renforcer la transparence des traitements.* Les personnes concernées doivent pouvoir utiliser les nouvelles technologies sans renoncer pour autant à leur liberté de décider quels données personnelles elles entendent mettre à disposition. Pour ce faire, la collecte et le traitement des données doivent bénéficier d'une meilleure transparence. Dans la loi actuelle, le devoir d'information dans le secteur privé n'existe que lorsque des données sensibles sont collectées et des profils de la personnalité constitués. Il s'agirait d'étendre cette obligation à toutes les catégories de données, comme c'est déjà le cas dans le secteur public. La personne concernée devrait également être informée du fait qu'une décision l'affectant a été prise de manière purement automatisée, à savoir sans intervention humaine, et pouvoir donner son point de vue. Le projet de révision devrait également introduire l'obligation de notifier les violations de données au PFPDT et d'étendre les informations à fournir lorsque la personne concernée exerce son droit d'accès.

4. *Assurer un meilleur contrôle et une meilleure maîtrise sur les données une fois celles-ci divulguées.* Le droit à l'oubli, qui peut déjà être déduit implicitement des art.15 et 25 LPD, serait explicité en mentionnant expressément un «droit à l'effacement». Il est également envisagé d'établir un mécanisme alternatif de règlement des conflits, qui permettrait aux personnes concernées de faire valoir leurs droits sans nécessairement devoir se lancer dans une procédure risquée et coûteuse.

5. *Renforcer les pouvoirs du PFPDT.* Il est envisagé de conférer au préposé le pouvoir de rendre des décisions, comme le prévoient les

réformes au niveau européen et comme la Suisse y a été invitée dans le cadre de l'évaluation Schengen de 2014. Actuellement, le PFPDT ne peut émettre que des recommandations. Il a ensuite la possibilité de les porter devant les autorités judiciaires si elles ne sont pas suivies. Ce sont là des compétences assez faibles, comparées à celles dont disposent les autorités de contrôle des autres pays européens et les autres organes de surveillance de la Confédération, qui ont le plus souvent un pouvoir décisionnel. Le PFPDT pourrait ainsi rendre une décision interdisant ou suspendant le traitement, ou encore enjoignant à son responsable de prendre les mesures qui conviennent. Il serait même habilité, dans certains cas, à prononcer des sanctions. Ses décisions pourraient faire l'objet d'un recours.

Les travaux législatifs sont actuellement en cours. Le catalogue de mesures ci-dessus n'est nullement exhaustif ou définitif. Le DFJP reste notamment libre d'examiner d'autres possibilités ou d'en abandonner certaines, en fonction des réformes européennes. Relevons par ailleurs, au vu du nombre d'interventions parlementaires déposées au niveau fédéral (initiatives parlementaires, motions, postulats), que la problématique de la protection des données trouve un relais important dans le monde politique depuis quelques années.



**Camille Dubois**

Unité organisationnelle Projets et méthode législatifs,  
Office fédéral de la justice (OFJ), Berne

4 Projet de directive relative à la protection des personnes physiques à l'égard du traitement des données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière ou d'exécution de sanctions pénales. Cette directive est destinée à remplacer l'actuelle 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).

5 Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (RS O.235.1).

6 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 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.

7 Esquisse d'acte normatif relative à la révision de la loi sur la protection des données – Rapport du groupe d'accompagnement Révision LPD du 29 octobre 2014.