de Preux
AVOCATS

NEWSLETTER MAI 2017

RÉVISION DE LA LOI SUR LA PROTECTION DES DONNÉES

Répercussion en matière de communication de données à l'étranger

INTRODUCTION

Le 4 avril dernier se terminait la consultation du Conseil fédéral sur son avant-projet de révision totale de la Loi fédérale sur la protection des données.

Cette révision a pour objectif de **renforcer** la législation existante, notamment au travers d'une amélioration de la **transparence** et en donnant un meilleur **contrôle** aux personnes sur le traitement de leurs données personnelles[1].

Cette révision doit également prendre en compte les réformes au **niveau européen**[2].

Ces dernières années, en matière de communication de données à l'étranger, la transmission des noms des employés de banque dans le cadre du litige fiscal avec les Etats-Unis a fait grand bruit.

Les banques invoquaient l'intérêt public prépondérant pour justifier du transfert de données dans le cadre des accords de non poursuite conclus avec le *Department of Justice* américain (DOJ).

La jurisprudence récente des tribunaux suisses a nié l'existence d'un tel motif justificatif[3].

Nous présenterons ici une brève analyse des **conséquences** que pourrait avoir la nouvelle loi en matière de **communication de données à l'étranger**.

I. PRINCIPE DE BASE

Le nouvel article 5 de l'avant-projet de Loi sur la protection des données (ci-près AP-LPD), intitulé « *communication de données personnelles à l'étranger* » reprend, pour l'essentiel l'article 6 de la loi actuellement en vigueur.

L'alinéa 1 pose le principe selon lequel **aucune donnée** ne peut être communiquée à l'étranger si la **personnalité** des individus concernés devait s'en trouver gravement **menacée**.

Par contre, des données pourraient être communiquées à l'étranger si le Conseil fédéral constate que la législation de l'Etat concerné assure un **niveau de protection adéquat** (art. 5 al. 2 AP-LPD), sous réserve des principes édictés à l'art. 4 AP-LPD[4].

Dans ce deuxième alinéa réside une nouveauté. La **compétence** de déterminer l'adéquation de la législation étrangère en matière de protection des données reposera désormais sur le **Conseil fédéral**.

Par le biais d'une ordonnance, avec une portée juridiquement contraignante, celui-ci

[1] *Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales* du 21 décembre 2016, p.6.
[2] *Directive (UE) 2016/68 et Règlement (UE) 2016/679 et modernisation de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*
[3] Cf. notamment l'arrêt du Tribunal fédéral du 22 septembre 2016, 4A_83/2016.
[4] Principes de licéité, de bonne foi, de proportionnalité, d'exactitude des données et de la finalité déterminée et clairement reconnaissable du traitement de données.

Genève
2, rue Pedro-Meylan
CH-1208 Genève
tel: +41 (0)22 700 51 52 ▪ fax: +41 (0)21 700 51 53

Lausanne
22, rue du Petit-Chêne 22 ▪ Case postale 5890
CH-1002 Lausanne
tel: +41 (0)21 312 59 40 ▪ fax: +41 (0)21 312 59 41

établira donc une **liste « positive »** des Etats disposant d'une législation assurant un niveau de protection adéquat (al. 7).

Il devrait être précisé dans l'ordonnance qu'elle sera **mise à jour** régulièrement[5].

Lorsqu'un Etat étranger ne figurera pas sur la liste du Conseil fédéral, cela pourra signifier soit (1) que celui-ci n'a pas encore évalué la législation de ce pays, soit (2) qu'il est arrivé à la conclusion que la loi nationale ne remplit les exigences pour qu'il puisse constater un niveau de protection adéquat[6].

Dans la situation actuelle, il incombe au maître du fichier, soit celui qui entend transmettre des données à l'étranger, de vérifier si la législation de l'Etat concerné assure un niveau de protection adéquat.

Le préposé fédéral à la protection des données établit une liste indicative servant de référence pour déterminer les Etats qui remplissent cette exigence (art. 7 de l'Ordonnance relative à la loi fédérale sur la protection des données ; OLPD)[7].

Il est intéressant de noter que les **Etats-Unis** figurent parmi les pays ne disposant pas d'une législation assurant un niveau de protection adéquat, sous réserve des entreprises privées qui ont adhéré au *Privacy Shield* et qui apparaissent sur la liste du Département américain du commerce. Toutefois, dans le contexte politique actuel, certaines craintes ont été exprimées au sujet de l'application de cet accord.

II. LES GARANTIES D'UN NIVEAU DE PROTECTION APPROPRIÉ

En l'absence d'une décision du Conseil fédéral, des données personnelles pourraient malgré tout être communiquées à l'étranger lorsqu'un niveau de protection approprié est garanti (art. 5 al. 3 AP-LPD) par :

- **Un traité international** (let. a) : il peut s'agir tant d'une convention portant sur la protection des données, que de tout autre accord international qui prévoit un échange de données. Sont notamment visés ici les accords de double-imposition.

- **Des garanties spécifiques** (let. b) : dans le secteur privé, il peut s'agir de clauses contractuelles entre le responsable du traitement et le destinataire qui garantissent une protection des données appropriées; dans le secteur public, l'organe fédéral peut, lorsqu'il accorde sa coopération à un Etat étranger, lui fixer des conditions à respecter en matière de protection des données. Ces garanties doivent être préalablement communiquées au préposé qui dispose d'un délai de 30 jours pour indiquer ses éventuelles objections au responsable du traitement (Art. 5 al.4 AP-LPD). Les garanties spécifiques ne valent que pour la communication prévue dans le contrat, un nouvel accord du préposé devant intervenir en cas de nouvelle communication[8].

- **Des garanties standardisées** (let. c): elles peuvent être élaborées par les personnes privées ou par les milieux intéressées, soit être établies ou reconnues par le préposé. Dans le premier cas, l'approbation préalable du préposé est nécessaire. Dans la seconde hypothèse, le préposé doit simplement être informé. Il peut s'agir de clauses contractuelles standardisées intégrées dans le contrat ou d'un code de conduite élaboré par le secteur privé. L'approbation du préposé doit être donnée dans un délai de six mois (art. 5 al. 5 AP-LPD). Une ordonnance devrait prévoir une obligation pour le préposé de publier une liste des garanties standardisées établies ou reconnues.

- **Des règles d'entreprises contraignantes** (let. d) : il s'agira de règles contraignantes pour les sociétés d'un même groupe d'entreprises qui devront préciser les transferts de données, leur catégorie, la finalité, les personnes concernées et les pays de destination. Lesdites règles

[5] *Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales* du 21 décembre 2016, p. 49.
[6] *op. cit.*, p. 47.
[7] https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=fr

[8] *Rapport explicatif concernant l'avant-projet de loi fédérale sur la révision totale de la loi sur la protection des données et sur la modification d'autres lois fédérales* du 21 décembre 2016, p. 48.

devront être préalablement approuvées par le préposé ou par une autorité chargée de la protection des données à l'étranger. Le préposé dispose d'un délai de 6 mois pour donner son approbation aux premières (art. 5 al. 5 AP-LPD), alors que pour les secondes, l'entreprise établie en Suisse devra simplement les communiquer au préposé.

L'article 5 AP-LPD reprend dans les grandes lignes l'actuel article 6 de la LPD. Toutefois, pour les lettres b, c et d, il s'agit d'un renforcement du droit en vigueur. L'**approbation du préposé** devient en effet indispensable, alors qu'actuellement, seule une obligation d'information figure dans la loi (art. 6 al. 3 LPD).

III. LES EXCEPTIONS

A l'instar du droit en vigueur, le projet de loi prévoit en son art. 6 al. 1 des exceptions pour lesquelles la transmission de données à l'étranger est possible, malgré l'absence d'une législation offrant un niveau de protection adéquat.

Les **exceptions** sont les suivantes :

- **Consentement de la personne concernée** (let. a) : la validité du consentement est subordonnée aux conditions de l'art. 4 al. 6 LPD. Il doit être donné librement, clairement et après que la personne concernée ait été dûment informée des risques du transfert. Lorsque le traitement concerne des données sensibles ou consiste en du profilage, le consentement doit être exprès.

- Le traitement est en **relation directe avec la conclusion ou l'exécution d'un contrat et les données concernent le cocontractant** (let. b) : cela correspond à l'article 6 al. 2 let. c de la LPD actuellement en vigueur.

- La sauvegarde d'un **intérêt public prépondérant** (let. c ch. 1) : cela correspond à l'art. 6 al. 2 let. d LPD actuellement en vigueur. L'intérêt public prépondérant comprend notamment la sécurité intérieure de la Suisse ou d'un Etat tiers[9].

- **La constatation, l'exercice ou la défense d'un droit devant une autorité judiciaire administrative** (let. c ch. 2) : cela correspond à l'actuel art. 6 al. 2 let. d, sous réserve de la formulation qui a été élargie puisqu'elle se limite aujourd'hui à la défense d'un droit « en justice ».

- La communication est nécessaire pour protéger la **vie ou l'intégrité corporelle** de la personne concernée ou d'un tiers (let. d).

- La personne concernée a rendu les données personnelles **accessibles à tout un chacun** et ne s'est pas opposée au traitement (let. e) : cette disposition correspond à l'actuel article 6 al. 2 let. f LPD.

- Les données proviennent d'un **registre prévu par la loi**, accessible au public ou à toute personne justifiant d'un intérêt légitime (let. f) : un certain nombre de conditions légales supplémentaires sont posées dans ce cas.

Des **règles de bonne conduite** pourront être édictées soit par le préposé, soit par les milieux intéressés qui pourront ensuite les soumettre à l'approbation du préposé.

Ces règles devraient permettre de **concrétiser** la loi et donner des solutions plus précises quant aux comportements à adopter[10].

IV. LES OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

En application des articles 13 à 15 AP-LPD, le responsable du traitement des données personnelles devra systématiquement **informer la personne concernée** au plus tard lors de la collecte des données.

Le responsable du traitement devra également mener une **analyse d'impact** préalable (art. 16 AP-LPD) et aura un **devoir de documentation** (art. 19 AP-LPD)

---

[9] *op. cit.,* p.49.
[10] *op. cit.*, p. 50.

Plus surprenant, il devra « **s'auto-dénoncer** » auprès du préposé en cas de violation des règles sur la protection des données (art. 17 AP-LPD).

V. MESURES ET SANCTIONS

Sur le **plan administratif**, le **préposé** aura un certain nombre de **mesures** à sa disposition.

L'article 41 AP-LPD lui confère le pouvoir de mener des **enquêtes** dès le moment où des indices font penser qu'un traitement de données pourrait être contraire à la loi.

Il pourra **ordonner** à une personne privée ou à un organe fédéral de **modifier ou de cesser** tout ou partie d'un traitement de données qui serait contraire à des dispositions de protections des données, ainsi qu'ordonner la **destruction** de données (art. 43 al. 1 AP-LPD).

Il pourra en outre **suspendre ou interdire** la **communication de données personnelles à l'étranger** si elle est contraire aux conditions des articles 5 et 6 commentés ci-dessus, ou à des dispositions spéciales d'autres lois fédérales (art. 43 al. 2 AP-LPD).

La nouvelle réglementation représente un **renforcement significatif du rôle du préposé** puisque la loi actuelle lui permet uniquement de formuler des recommandations de modifier ou de cesser un traitement. Si les recommandations du préposé ne sont pas respectées, il peut saisir le Tribunal administratif fédéral pour requérir le prononcé d'une décision contraignante (art. 29 LPD).

Les décisions du préposé seront sujettes à recours auprès du Tribunal administratif fédéral (art. 44 AP-LPD). Le préposé et la personne privée contre laquelle une enquête aura été ouverte sont les seuls à disposer de la qualité de parties, ce qui signifie que le dénonciateur ne pourra pas intervenir dans la procédure. Celui-ci aura alors intérêt à ouvrir une action civile en parallèle.

Contrairement à la législation européenne, le préposé n'aura **pas le pouvoir de prononcer lui-même des sanctions**. Ce point de la révision est vivement critiqué par la doctrine[11].

Le préposé aura par contre le **devoir de dénoncer** aux autorités pénales compétentes les **infractions** dont il a eu connaissance dans l'exercice de ses fonctions (art. 45 AP-LPD).

Les **sanctions pénales** sont prévues par les art. 50 et suivants AP-LPD.

Si la décision administrative prise par le préposé en application de l'article 43 AP-LPD n'est pas respectée, la personne qui a reçu la notification sera punie d'une **amende** en vertu de l'art. 50 al. 2 let. e AP-LPD.

La violation des articles 5 et 6 sera également sanctionnée pénalement (art. 50 al. 2 let. b et 51 al. 1 let. a AP-LPD).

En cas de **transmission de données à l'étranger en violation** de l'art. 5 al. 1 et 2 sans que les conditions de l'article 6 AP-LPD ne soient remplies, la personne privée sera punie sur plainte d'une **amende** pouvant aller **jusqu'à CHF 500'000.-,** ou CHF 250'000.- en cas de négligence (art. 51 al.1 let. a LPD).

Le **défaut d'information** de l'art. 17 AP-LPD sera punie de la même amende (art. 50 al. 3 let. b AP-LPD).

Le montant maximum de l'amende augmenterait donc fortement puisqu'il est aujourd'hui fixé à CHF 10'000.- (art. 106 al. 1 CP).

On peut noter que le Conseil fédéral a toutefois décidé de ne pas suivre le règlement européen, lequel prévoit des amendes administratives pouvant aller jusqu'à EUR 20 millions, respectivement jusqu'à 4% du chiffre d'affaires annuel mondial de l'entreprise[12].

Lorsque l'infraction est commise **dans une entreprise**, si l'amende ne dépasse pas **CHF 100'000.-** et que l'identification de la personne physique responsable au sein de l'entreprise nécessiterait des mesures d'instruction hors de proportion, l'entreprise elle-même pourra être **condamnée au paiement de l'amende** (art. 53 AP-LPD).

---

[11] Voir notamment l'article de Mes Sylvain MÉTILLE et David RAEDLER, paru dans la revue plaidoyer 2/17, p. 38 ss.

[12] Art. 83 du Règlement (UE) 2016/679

Enfin, **sur le plan civil**, la personne concernée pourra toujours **agir** en **protection de sa personnalité** sur la base des articles 28 et suivants du Code civil (renvoi de l'art. 25 AP-LPD). Il sera notamment possible de requérir du juge l'interdiction de la communication de données personnelles à des tiers.

L'AP-LPD entraînera une **modification du Code de procédure civile** (CPC). **Aucun frais judiciaires** ne seront prélevés, que ce soit en procédure de conciliation ou dans la procédure au fond, et le demandeur ne sera **pas tenu de fournir des sûretés**. La **procédure simplifiée** sera applicable aux procédures en matière de protection des données, quelle que soit leur valeur litigieuse (alors qu'actuellement seuls les litiges portant sur le droit d'accès aux données y sont soumis).

V. CONCLUSION

En matière de communication de données à l'étranger, les nouveautés apportées par le projet de loi du Conseil fédéral portent surtout sur le **poids des sanctions** en cas de violation des dispositions légales.

Le changement concerne aussi le **pouvoir décisionnel** laissé au **préposé** puisqu'il pourra approuver ou non les garanties sensées offrir une protection appropriée des données. Le préposé aura le pouvoir de prononcer des décisions administratives dont la violation sera punissable pénalement.

Les jurisprudences rendues ces dernières années par les tribunaux civils en matière de transmission de données à l'étranger continueront à s'appliquer, les exceptions permettant la transmission de données vers des Etats ne disposant pas d'un niveau de législation adéquat ne subissant pas de changement.

Le contenu de cette Newsletter ne représente pas un avis ou un conseil juridique. Un des avocats suivants se fera un plaisir de vous conseiller sur votre situation particulière:

A Genève :

Christian de Preux

Associé

christian.depreux@depreuxavocats.ch

Corinne Lepage

Avocate-stagiaire

corinne.lepage@depreuxavocats.ch

A Lausanne :

Pascal de Preux

Associé

pascal.depreux@depreuxavocats.ch

Marc-Henri Fragnière

Associé

mhfragniere@depreuxavocats.ch

Daniel Trajilovic

Collaborateur

daniel.trajilovic@depreuxavocats.ch

Marek Noyer

Avocat-stagiaire

marek.noyer@ depreuxavocats.ch