Transmission aux autorités américaines de données personnelles concernant des avocats suisses

M^e Alice Reichmuth Pfammatter, docteur en droit*

Traduction libre de la version allemande du 2 juin 2014

Remarques liminaires

A l'origine, cet avis de droit avait été établi lors de la publication de l'*US-Program for Non-Prosecution Agreements* (ci-après *NPA*) tendant au règlement du différend fiscal entre les banques suisses et les Etats-Unis.

Il s'adresse aujourd'hui aux avocats suisses confrontés à la transmission de données personnelles les concernant. En revanche, il n'examine ni le cas particulier des avocats intermédiaires financiers ni les transmissions de données dans une procédure d'entraide judiciaire.

Ce document, conçu sous la forme d'un vade-mecum, contient surtout des informations sur le droit de la protection des données. Il ne répondra donc pas à des questions typiquement bancaires ou financières. Enfin, il ne couvre pas tous les cas de figure et chaque membre de la FSA aura tout intérêt à examiner attentivement sa situation particulière.

* Préposée à la protection des données du canton de Fribourg, avocate-conseil chez *Kessler Wassmer Giacomini & Partner* à Schwytz et Wollerau.

Sommaire

de plusieurs moyens de droit (art. 15 al. 1er LPD, à mettre en relation avec les art. 28 et 28a CC) :

- Dépôt d'une demande selon la procédure ordinaire du CPC, après tentative de conciliation.
- Il peut être judicieux d'introduire immédiatement la procédure de conciliation → **chiffre 3.1**, éventuellement de requérir des mesures provisionnelles → **chiffre 3.2**

Vue d'ensemble des différentes catégories de données et leur éventuelle transmission :

Catégories de données	Transmission ?
Données de clients : Nom, n° de compte, n° AVS	Transmission formellement interdite dans le cadre du *NPA*, en raison du secret bancaire.
Eléments permettant d'identifier le client indirectement	Transmission implicitement interdite. Du côté de l'avocat : la transmission de ses données permet une identification indirecte du client et n'est donc pas couverte par les autorisations délivrées par le Conseil fédéral (cf. explications données plus bas).
Leaver lists : Données générales (virements avec indication du montant et du destinataire), mais sans donner le nom du client	Transmission en principe autorisée si aucune donnée personnelle du client. Transmission éventuellement interdite au regard de l'art. 273 al. 2 CP (secret d'affaires).

Les tiers ne sont pas protégés par le secret bancaire : Cas des avocats	Transmission autorisée sous réserve d'une violation du droit de la protection des données, notamment pour les motifs suivants : • Les données initialement recueillies en Suisse ne remplissent plus le même objectif à l'étranger. • Intérêt public : il n'est pas légitime de contraindre l'avocat à choisir entre « violer son secret professionnel en Suisse » et « éviter une poursuite pénale à l'étranger ». La transmission de données viole ainsi le principe fondamental du secret professionnel au sens de l'art. 13 LLCA, à mettre en relation avec l'art. 321 CP. • Proportionnalité : il n'y aucune adéquation entre les moyens mis en oeuvre (violer le secret professionnel de l'avocat en transmettant ses données personnelles, créant ainsi un dommage important pour lui) et le but poursuivi (déceler d'éventuelles soustractions d'impôt).

1. Contexte

1.1 *US-Program for Non-Prosecution Agreements (NPA) or Non-Target Letters for Swiss Banks*

Le 29 août 2013, le Département de la justice américaine (ci-après DOJ) a publié un programme visant à régler le différend fiscal opposant les banques suisses aux Etats-Unis. Ce programme énumère des prescriptions et des conditions devant permettre à toutes les banques suisses – qui ne sont pas impliquées dans une procédure pénale en matière fiscale avec les Etats-Unis – de régler directement leur cas avec les autorités américaines compétentes. Pour régulariser leur situation, les banques peuvent ainsi demander un *NPA* conformément au chiffre II du programme (catégorie 2) ou une *Non-Target Letter* conformément aux chiffres III (catégorie 3) et IV (catégorie 4)[1].

[1] Communication FINMA 50 (2013) du 30 août 2013.

Selon les informations données par le Secrétariat d'Etat aux questions financières internationales (ci-après SIF), la solution trouvée se compose de trois éléments cardinaux: le *joint statement* des gouvernements suisse et américain, le programme unilatéral américain auquel les banques peuvent participer volontairement et, côté suisse, les autorisations du Conseil fédéral selon l'art. 271 CP qui permettent aux banques de coopérer[2].

Au chiffre 5 du *joint statement* entre le DOJ et le DFF du 29 août 2013, on retient ce qui suit (traduction libre par le SIF)[3] :

5. Compte tenu de l'importance accordée par chaque partie à la protection des données personnelles et de la vie privée des personnes telle que requise par leurs lois respectives, les signataires entendent, en cas d'échange de données personnelles, n'utiliser ces données que dans le cadre de procédures visant le respect du droit (qui peuvent comprendre des actions réglementaires) engagées aux Etats-Unis ou autorisées par le droit américain. Les données personnelles ne peuvent être conservées qu'aussi aussi longtemps que nécessaire pour ces buts.

Autorisations selon l'art. 271 CP données par le Conseil fédéral aux banques suisses

Les banques qui souhaitent participer au *NPA* et coopérer selon le droit suisse avec les autorités américaines doivent obtenir une autorisation du Conseil fédéral selon l'art. 271 ch. 1er CP[4]. Celle-ci fournit une protection contre la poursuite pénale des actes illicites commis en faveur d'un Etat étranger.

Conçue sous la forme d'une décision-modèle préparée par le SIF en date du 3 juillet 2013, l'autorisation du Conseil fédéral définit tout d'abord les données pertinentes qui se rattachent à un citoyen américain (en particulier les indications personnelles et autres documents qui permettent de l'identifier), les *leaver lists*, ainsi que les données personnelles de collaborateurs de la banque et de tiers (p. ex. l'avocat comme nous le verrons plus bas).

La décision-modèle exclut du *NPA* toutes les données de clients. Celles-ci ne pourront être transmises que dans le cadre d'une procédure d'entraide

[2] http://www.sif.admin.ch/00488/index.html?lang=fr&msg-id=50049
[3] http://www.news.admin.ch/NSBSubscriber/message/attachments/31814.pdf
[4] Le SIF a publié sur cette décision-modèle, ainsi qu'une note explicative sur http://www.sif.admin.ch/00488/index.html?lang=fr&msg-id=50049.

judiciaire fondée sur une convention de double imposition, comme le publie le SIF[5] sur son site[6].

L'autorisation précise ensuite un certain nombre d'obligations, notamment celles d'informer les collaborateurs de la banque ou les tiers de la transmission de leurs données personnelles, de leur indiquer les voies de droit et de ne livrer les données qu'après entrée en force d'une décision judiciaire[7]. Ces exigences font partie intégrante de l'autorisation et leur respect est nécessaire pour supprimer le caractère illicite de l'art. 271 ch. 1er CP. Enfin, l'inobservation de ces exigences est constitutive de l'art. 292 CP.

Recommandations du préposé fédéral à la protection des données pour la transmission de données personnelles aux autorités américaines

Le 15 octobre 2012 déjà, le préposé fédéral à la protection des données publiait, à l'attention des banques concernées par le différend fiscal avec les Etats-Unis, des recommandations pour une transmission de données personnelles conforme au droit helvétique. Dans sa note informative du 20 juin 2013, il énumérait les principes généraux à garantir par les banques qui allaient éventuellement transmettre des données personnelles[8]. Le préposé a notamment rappelé que la transmission de données devait respecter le principe de la proportionnalité (art. 4 al. 2 LPD[9]), disposition qui s'applique également aux personnes ayant organisé, suivi ou surveillé des relations d'affaires avec des citoyens américains. Le préposé fédéral a ensuite exigé que les personnes concernées (art. 4 al. 2 et 4 LPD) soient préalablement informées de la possibilité d'accéder en temps utile à leurs données personnelles (art. 8 LPD). En outre, lorsque la personne concernée s'oppose à cette transmission, la banque a l'obligation de faire une pesée des intérêts en cause (art. 13 LPD) et d'informer toutes les parties de leurs droits.

---

[5] Contact : info@sif.admin.ch
[6] http://www.sif.admin.ch/themen/00502/00806/index.html?lang=fr
[7] Ch. 1.4 de la décision-modèle
[8] Recommandations du préposé fédéral à la protection des données du 15 octobre 2012 aux banques concernées par le différend fiscal (en allemand) : http://www.edoeb.admin.ch/datenschutz/00628/00663/index.html?lang=de
[9] Loi fédérale sur la protection des données du 19 juin 1992 (LPD), RS 235.1

1.2 Quelles sont les données concernées ?

A la lumière de la décision-modèle[10] selon l'art. 271 ch. 1er CP, on retiendra les données et documents suivants :

- *L'autorisation s'applique aux renseignements et documentations d'ordre général concernant les pratiques commerciales de la requérante, ainsi qu'aux renseignements sur les relations d'affaires impliquant une personne américaine ;*
- *Elle ne s'applique pas aux données des clients des banques. Celles-ci ne peuvent être transmises aux autorités américaines que sur la base d'une entraide judiciaire ;*
- *Elle s'applique aux leaver lists qui comprennent des données non personnelles ayant trait à la clôture de comptes et au transfert consécutif des fonds concernés dans une autre banque ;*
- *Elle s'applique aux données personnelles de membres du personnel qui ont organisé, suivi ou surveillé des relations d'affaires, ainsi que celles de tiers qui ont agi d'une manière similaire pour des relations d'affaires de ce genre.*

Si ces conditions sont remplie, la décision-modèle autorise les banques à livrer des données personnelles (p. ex. celles de l'avocat ; cf. plus bas), en plus d'informations plus générales. Comme mentionné plus haut, elle exclut en revanche toutes données de clients qui doivent, cas échéant, être transmises par un autre canal.

Données de l'avocat

Les données transmises selon la décision-modèle du Conseil fédéral peuvent également inclure des données personnelles de l'avocat s'ils sont eux-mêmes qualifiés par les banques de « tiers ». Les données de l'avocat sont notamment les suivantes : son nom, son IDE, son adresse postale ou électronique, ses numéros de téléphone, mais aussi – très important – la correspondance postale et électronique de l'avocat actif pour des clients américains[11]. Les *leaver lists* précitées contiennent souvent ce type d'informations.

---

[10] http://www.sif.admin.ch/00488/index.html?lang=de&msg-id=50049

[11] Les numéros AVS, de l'IDE, du passeport, de la carte de crédit, du compte bancaire ou d'autres numéros identifiables sont eux aussi des données personnelles au sens de l'art. 3 let. a LPD, dès lors qu'ils permettent d'identifier la personne concernée (cf. Rosenthal, ch. 21 ad art. 3 LPD).

Données du client

Il est difficile de déterminer dans quelle mesure les « informations pertinentes »[12] exigibles par le DOJ peuvent elles aussi contenir des données de client, à plus forte raison que le ch. II.D.2 du programme américain[13] exige plusieurs données pour chaque compte (solde, nombre d'ayants droit, nom et fonction du tiers en contact avec le client, etc.). Ces « informations pertinentes » permettent-elles d'identifier le client américain ? Une identification indirecte n'est jamais exclue, d'autant plus que – conformément aux lignes directrices de la décision-modèle du Conseil fédéral – le *NPA* n'exclut finalement que les « données bancaires du client » (nom, adresse, n° AVS ou du compte). En d'autres termes, tout le reste peut potentiellement être transmis. La doctrine est quant à elle divisée pour déterminer jusqu'à quel point une personne peut être identifiée[14]. En raison de l'intérêt des autorités américaines concernées par le programme, il est prudent de partir de l'idée que la plupart des personnes seront finalement identifiées. Pour l'avocat, les exigences sont donc particulièrement élevées : pour respecter en tout temps son secret professionnel, il devra se demander quelles sont les données qu'il est en droit de fournir et si celles-ci ont été rendues suffisamment anonymes.

1.3 Confronté à une transmission de ses données personnelles, y a-t-il péril en la demeure ?

Dans sa décision-modèle, le Conseil fédéral prévoit que la législation suisse et les règles de la protection des données devront être respectées. La violation du droit positif, donc également celle des principes généraux de la LPD, entraîne la sanction pénale de l'art. 292 CP.

Se pose ensuite la question de la nécessité d'agir rapidement, en particulier pour exercer son droit d'accès aux données personnelles et celui de s'opposer à la transmission par les banques suisses. Il s'agira avant tout d'examiner si la personne concernée peut faire valoir ses droits en temps utile. Dans ce contexte, on imagine fort bien que les banques qui se sont

[12] Selon ch. 1.1 de la décision-modèle.
[13] http://www.justice.gov/opa/pr/2013/August/13-tax-975.html
[14] Rosenthal, notes 24 s. ad art. 3 LPD.

engagées à participer au programme sont soumises à des délais particulièrement courts.

Au vu de ce qui précède, l'avocat devra répondre aux questions suivantes, en tenant compte de l'ensemble des circonstances du cas particulier :

- Les droits d'accès et de consultation des données personnelles – tels qu'ils sont prévus par la législation suisse – ont-ils été exercés pour que la personne concernée puisse s'opposer à la transmission envisagée ?
- Cette personne peut-elle ensuite saisir directement un juge ? Si oui, quelles sont les conditions ?
- Est-il possible de prévoir avec le client un moyen alternatif qui lui donne satisfaction ?

1.4 Scénarios possibles

Il existe plusieurs scénarios dans lesquels les avocats pourront être identifiés sur la base de documents bancaires et qui seront ainsi confrontés à la transmission de leurs données personnelles. Voici les cas les plus fréquents :

- (1) Les avocats qui représentent professionnellement des clients américains (p. ex. des exécuteurs testamentaires) et dont le nom figure parmi les données bancaires des clients.
- (2) Les avocats qui ont représenté professionnellement des établissements bancaires. Leurs noms peuvent apparaître dans les données ou informations générales des affaires qu'ils ont traitées.
- (3) Mais aussi les avocats dont le nom figure en dehors de la représentation d'un client.

En revanche, ne sont pas concernés les avocats autorisés à gérer des transactions financières ou dans une relation de travail avec une personne autorisée par la FINMA.

Sans indication contraire, les considérations suivantes entrent dans les catégories (1) à (3).

2. Arguments tirés du droit de la protection des données

La transmission de données qui concernent l'avocat, en qualité de « tiers » selon le programme américain, constitue des données personnelles telles que définies à l'art. 3 let. a LPD. Ces données sont en effet traitées (au sens où l'entend la LPD) afin de les transmettre à l'étranger[15].

2.1 La transmission de données à l'étranger est-elle licite ?

Conformément à l'art. 6 LPD, « aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée. » Le traitement des données doit par ailleurs être licite (art. 4 al. 1er LPD) et être justifié. L'intérêt public de l'art. 6 al. 2 let. b LPD ne suffit pas, à lui seul, pour considérer que ces exigences sont remplie[16].

Ainsi, en transmettant des données aux autorités américaines, il est porté atteinte à la personnalité du client et de l'avocat concerné. Les motifs justificatifs de l'art. 13 LPD, qui permettent de porter atteinte aux intérêts de la personne concernée, ne nous semblent pas donnés.

Le **traitement des données est illicite** dans les cas suivants :

Du côté du client :

- Sous le titre marginal « Service de renseignements économiques », l'art. 273 al. 2 CP sanctionne notamment le fait de divulguer à un organisme ou une autorité officielle à l'étranger des secrets d'affaire[17]. En même temps, le Conseil fédéral délivre des autorisations aux banques pour leur permettre de coopérer avec les autorités américaines. Ces autorisations sont délivrées sur la base de l'art. 271 CP et ne supprime l'illicéité des actes que pour cette disposition. Pour le surplus, la décision-modèle du Conseil fédéral du 3 juillet 2013 précise explicitement qu'elle « ne dispense cependant

[15] Comme traitement de données particulièrement sensible, dès lors que les données personnelles passent à un autre cercle de traitement.
[16] Si des données personnelles sont transmises à l'étranger, elles ne sont plus soumises au droit suisse.
[17] Cf. Rosenthal, notes 2 s. ad art. 273 CP.

pas du respect des autres dispositions du droit suisse, notamment de la prise en compte du secret d'affaires et du secret bancaire existants, des dispositions sur la protection des données et des obligations de l'employeur ». Au vu de ce qui précède, l'autorisation du Conseil fédéral n'autorise pas la banque à violer son secret bancaire par des éléments d'identification indirecte (en particulier par le biais des données personnelles de l'avocat). Le fait que les données ne sont pas communiquées « directement » ne modifie en rien ce qui vient d'être exposé. Ainsi, lorsque les *leaver lists* permettent d'identifier indirectement le client, la transmission de données personnelles contrevient au droit suisse.

- En recueillant des données et en envisageant de les transmettre aux autorités américaines, les données établies dans la relation contractuelle entre la banque et le client (et son avocat) sont affectées à un nouveau but. Ceci contrevient au principe défini par l'art. 4 al. 3 LPD, à savoir que « les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances ». Dans le cas particulier, la banque collecte des données personnelles uniquement dans le cadre de ses activités bancaires, dans lesquelles elle dispose d'un savoir-faire et d'une compétence spéciale. Or, par définition, l'avocat n'est pas un banquier : son rôle d'expert consiste essentiellement, dans le mandat qu'il accomplit, à s'assurer de la bonne exécution du contrat entre son client et la banque. Les données personnelles du client et de l'avocat sont ainsi collectées et traitées dans un but précis, tel que l'entend la LPD. Or, le traitement ultérieur des données par les Etats-Unis, que ce soit par transmission à un « examinateur indépendant » ou par transfert direct aux autorités américaines, répond à des objectifs complètement différents de ceux initialement définis. Et ce changement d'affectation n'était aucunement prévisible.
- Enfin, il convient de vérifier, dans chaque cas particulier, si les données ont été recueillies ou transmises conformément aux principes de la bonne foi et de la proportionnalité (art. 4 al. 2 LPD), en tenant p. ex. compte des pratiques commerciales antérieures (correspondance, garanties données par la banque, etc.).

Du côté de l'avocat :

La situation de l'avocat est incertaine : dans les *leaver lists* que les banques doivent soumettre aux autorités américaines, il y a effectivement les « données non personnelles » prévue par la décision-modèle du Conseil fédéral. Or, ces « données non personnelles » permettent elles aussi d'identifier sans grande difficulté une personne lorsque les données n'ont pas été rendues suffisamment anonymes. C'est typiquement le cas lorsque les listes contiennent le nom de l'avocat qui a traité l'affaire. L'avocat se trouve ainsi dans une situation particulièrement inconfortable : d'une part, il est lié par le secret professionnel, d'autre part, il est passible de poursuites pénales (aussi bien s'il ne coopère pas avec les autorités américaines que s'il viole le secret professionnel de l'art. 321 CP). En outre, en sa qualité de « tiers », il n'est en rien protégé par les autorisations du Conseil fédéral, à l'inverse des employés de la banque.

Quelques arguments :

- La transmission de données concernant l'avocat permet également une identification indirecte du client. En effet, les données liées au mandat sont de nature à divulguer qui est la personne représentée. Or, comme mentionné plus haut, les données qui tombent sous le coup du secret bancaire ne sont pas couvertes par les autorisations du Conseil fédéral.
- L'art. 273 CP protège, entre autres, les secrets définis par la loi. La transmission de *leaver lists* qui contiennent les données d'avocats peut éventuellement violer les secrets d'affaires[18]. L'art. 273 CP ne constitue pas une protection primaire des secrets d'affaires, mais n'a de sens que si le secret en question a déjà été garanti ailleurs[19]. Avec une transmission des données à l'étranger, la banque divulgue des secrets à une organisation étrangère. En d'autres termes, la banque se rend coupable de l'art. 273 al. 2 CP, étant toutefois précisé qu'il appartiendra à l'avocat de prouver un dommage découlant directement de cette violation du secret (arrêt du TPF du 25 avril 2013, BB.2012.133).

[18] Rosenthal, note 41 ad art. 273 CP.
[19] Rosenthal, note 41 ad art. 273 CP.

Arguments découlant du droit de la protection des données :

- La transmission de données est illicite, dès lors qu'elle contrevient aux principes généraux du traitement des données, en particulier à la lumière de l'art. 4 LPD : lorsque les données sont transmises contre la volonté de l'avocat concerné, la LPD est violée. Par ailleurs, ce traitement de données n'est pas conforme au but visé (cf. art. 4 al. 2 LPD et les explications données ci-dessus).
- La transmission de données ne répond pas à un intérêt public : dans la pesée des intérêts, essentielle pour déterminer si une transmission des données est justifiée ou non, la garantie du secret professionnel de l'avocat prime sur toute autre considération. Contraindre l'avocat à choisir entre violer son secret professionnel ou faire l'objet de poursuite pénale est dénué de toute pertinence et de tout fondement juridique. La transmission de données viole le principe-même du secret professionnel de l'art. 13 LDIP, à mettre en relation avec l'art. 321 CP. On rappellera à ce sujet qu'un avocat condamné pour violation du secret professionnel perd son droit d'exercer en raison de sa radiation au registre.
- En outre, la transmission de données est contraire au principe de la proportionnalité, dans la mesure où les conséquences de la communication du nom de l'avocat sont totalement disproportionnées par rapport au but visé, à savoir déceler d'éventuelles soustractions d'impôt. On part de l'idée que les avocats ne violeront pas leurs obligations professionnelles, de sorte que la mesure n'atteindra de toute façon pas son but.
- Enfin, demander à l'avocat de violer ses obligations professionnelles est d'autant plus disproportionné que les conséquences aux États-Unis sont difficiles à délimiter. En effet, conformément au ch. 5 du *joint statement*, les Etats-Unis entendent « n'utiliser ces données que dans le cadre de procédures visant le respect du droit (qui peuvent comprendre des actions réglementaires) engagées aux Etats-Unis ou autorisées par le droit américain. ». Devant de telles imprécisions, la transmission de données est totalement indéfendable.

2.2 Informations données par la banque

La décision-modèle du Conseil fédéral prévoit d'informer en temps utile les personnes touchées par une transmission des données. Au regard du droit de la protection des données, cette information doit être suffisamment claire et précise pour que l'intéressé puisse avoir une idée de l'étendue et de l'importance des données qui seront transmises. Dans tous les cas, cette information **devrait** déclencher une réaction de la personne concernée, dans l'intérêt de celle-ci, en particulier pour qu'elle :

- s'oppose immédiatement à la transmission prévue (2.3),
- exerce son droit d'accès aux données personnelles, en particulier en demandant des informations précises sur l'étendue, la nature et la période de référence des données qui seront transmises (2.4) ou qu'elle
- dépose sans tarder une demande judiciaire (3).

2.3 Opposition à la transmission des données

Il est recommandé de **s'opposer immédiatement** à la transmission des données. Comme exposé plus haut, celle-ci contrevient aux principes élémentaires de la protection des données et, d'une manière plus générale, au droit suisse. Rien ne permet de justifier une telle atteinte à la personnalité. En effet, à partir du moment où il n'y a pas consentement, il n'existe aucun intérêt prépondérant (privé ou public) ni de disposition légale qui justifie cette violation du droit (art. 13 LPD). Lorsque la personne concernée s'oppose à la transmission de ses données, la banque aura pour obligation légale de faire une pesée des intérêts au sens de l'art. 13 LPD. La question de savoir si les banques le font systématiquement reste ouverte. En revanche, ce qui est sûr, c'est que la personne devra systématiquement faire appel à un juge si la banque maintient sa volonté de transmettre les données.

2.4 Droit d'accès aux données

Lorsque les circonstances laissent à penser, eu égard à la pratique antérieure ou aux garanties données par la banque, que celle-ci ne transmettra pas les données avant clarification de la situation et épuisement

des moyens de droit, la personne concernée peut faire valoir son droit d'accès aux données (art. 8 à 10 LPD)[20].

S'agissant du droit d'accès, de quels éléments faut-il tenir compte ?

- La personne concernée peut exiger de la banque qu'elle lui communique toutes les données la concernant (art. 8 LPD). Ce droit porte également sur l'origine des données, le but et éventuellement la base juridique du traitement, les catégories de données personnelles, les personnes qui figurent dans le même fichier et les éventuels destinataires des données personnelles.
- Sur le principe-même de ce droit, la personne concernée n'a pas à remplir des conditions particulières pour accéder aux données la concernant.
- En revanche, conformément à l'art. 1er al. 3 OLPD, les modalités d'accès doivent être définies d'entente avec le maître du ficher (en l'occurrence la banque). Il est recommandé de consulter directement sur place les documents destinés aux autorités américaines, et d'en demander des copies ou des extraits.
- Il arrive fréquemment que des lettres standard soient utilisées par les banques. Celles-ci ne font qu'énumérer les différentes catégories possibles de documents et le destinataire final des données transmises n'est pas clairement identifiable, typiquement lorsque le terme générique de « *US Departement of Justice or other authorities* » est utilisé. La personne concernée doit ensuite être informée sur la façon dont les banques vont transmettre les données personnelles (sous forme de codes, en caviardant le texte, etc.). Elle doit aussi pouvoir identifier les noms d'emprunt et prendre connaissance à la fois des documents caviardés et non caviardés, puis en lever copie ou à tout le moins recevoir des extraits[21]. La personne concernée doit ainsi reconnaître l'étendue et la portée des données qui seront transmises. Il faut partir de l'idée que les informations liées à un compte déterminé – même si le numéro de celui-ci ou le nom du client ne sont pas explicitement mentionnés – permettront

[20] Ainsi que les art. 1er et 2 de l'Ordonnance fédérale sur la protection des données du 14 juin 1993 (OLPD).

[21] C'est en tout cas le droit que les tribunaux zurichois ont reconnu à un banquier à la retraite (décision du tribunal de district de Zurich du 14 octobre 2013, CG120124-L/U ; arrêt du tribunal supérieur de Zurich du 28 février 2014)

finalement d'identifier sans difficulté le titulaire du compte en cas de procédure d'entraide judiciaire.

Toujours par rapport au droit d'accès prévu par la LPD, il convient notamment de se poser les questions suivantes :

- La banque permet-elle d'exercer ce droit d'accès aux données suffisamment tôt, de sorte que la personne concernée puisse réagir adéquatement ?
- La banque a-t-elle fourni à la personne concernée l'ensemble des données, respectant ainsi son droit à recevoir une information complète sur les données qui seront transmises ?
- Quelle est l'étendue des données personnelles transmises (s'agit-il de plusieurs personnes, de plusieurs documents, de plusieurs listes, etc.).
- Quels sont les documents précis qui seront finalement transmis dans le cas particulier ?
- Quelle est la période de référence (début et fin) des données personnelles et des documents qui seront transmis ?
- Les données personnelles, y compris les numéros de compte et les éléments permettant d'identifier des personnes, ont-elles toutes été caviardées ?
- Les données personnelles ont-elles été rendues suffisamment anonymes, excluant ainsi tout rattachement avec la personne concernée[22] ?
- Ou s'agit-il de données personnelles avec un nom d'emprunt qui permettent, au moyen d'une clé ou d'un identifiant personnel, de tirer des conclusions sur la personne concernée ?
- Qui sont les destinataires (ou catégories de destinataires possibles) des données transmises ? Les données personnelles sont-elles transmises à un *independent examiner* ? Si oui, des données personnelles ont-elles déjà été divulguées à l'étranger ?
- Des données supplémentaires ont-elles été obtenues par des tiers ? Quelle est la source de ces données?
- Dans quel but les données personnelles ont-elles été transmises ?

[22] Pour la différence entre « rendre anonyme » et « utiliser des noms d'emprunt », cf. Rosenthal, note 36 ad art. 3 LPD.

- Si des codes ont été utilisés, la personne concernée peut-elle les décoder ?
- Les données personnelles qui seront transmises sont-elles correctes ?

Si aucune donnée n'est disponible, la banque doit là aussi en informer la personne concernée[23].

Lorsque la personne concernée constate que ses données la concernant sont incorrectes, elle peut en demander la rectification immédiate (art. 5 al. 2 LPD). Ce droit peut être exercé en tout temps, oralement ou par écrit.

Si le droit à l'accès aux données personnelles est refusé ou limité, la personne concernée n'a pas forcément intérêt à faire valoir ce seul point litigieux devant un tribunal[24]. Dans ce cas, il paraît plus judicieux de déposer directement une demande concluant à interdire la transmission des données personnelles.

3. Moyens de droit

Si la banque persiste dans son intention de transmettre des données personnelles, il ne reste à la personne concernée que la voie judiciaire prévue par l'art. 15 al. 1er LPD.

A son chiffre 1.4.c, la décision-modèle du Conseil fédéral rappelle ce droit d'intenter action selon l'art. 15 LPD et prévoit expressément qu'une éventuelle transmission des données ne pourra avoir lieu qu'après entrée en force de la décision rejetant la demande.

3.1 Demande

La personne concernée peut également intenter une action pour atteinte à la personnalité conformément aux art. 28 et 28a CC. La personne concernée peut notamment conclure à l'interdiction de transmettre des données par la banque aux autorités américaines.

---

[23] Au sujet du droit d'accès, cf. Rosenthal/Jöhri, Commentaire sur la LPD, notes 13 ss ad. art. 8 LPD.

[24] La procédure simplifiée du CPC qui s'applique au droit d'accès aux données (cf. art. 15 al. 4 LPD, à mettre en relation avec l'art. 243 al. 2 let. d CPC).

For : le tribunal du domicile ou du siège de l'une des parties (art. 20 let. a et d CPC)

Procédure : ordinaire selon les art. 219 ss CPC et introduite par une tentative de conciliation selon les art. 202 ss CPC.

Conclusions : elles doivent être formulées en tenant compte du cas particulier. Il s'agira avant tout de faire interdire la transmission de données personnelles aux autorités américaines qui est en soi une atteinte à la personnalité[25]. Selon les circonstances, des conclusions plus détaillées pourront être utiles.

Il est également recommandé d'exiger les mesures d'exécution prévues à l'art. 343 al. 1er CPC, sous commination de l'art. 292 CP.

Légitimation : la personne concernée, telle qu'elle est définie à l'art. 3 let. b LPD, jouit de la légitimation active.

La banque, qui agit par ses organes, possède la légitimation passive. Elle découle de l'atteinte à la personnalité du demandeur.

Intérêt juridiquement protégé : pour interdire une atteinte imminente, la personne concernée doit démontrer un intérêt juridiquement protégé. Elle a un intérêt juridiquement protégé si le défendeur n'admet pas l'illicéité de l'acte contesté (ATF 124 III 74).

3.2 Mesures provisionnelles et superprovisionnelles

Il peut également être judicieux de requérir des mesures provisionnelles ou superprovisionnelles visant à interdire à la banque de transmettre aux autorités américaines des documents incluant des données personnelles. Ces mesures peuvent d'ailleurs être requises avant la litispendance (art. 263 CPC). Cette procédure peut s'avérer particulièrement utile, notamment

[25] Cas échéant, il y aura lieu d'exiger que les données recueillies illicitement soient détruites (cf. Commentaire bâlois, Rampini, note 8 ad art. 15 LPD).

lorsqu'il faut s'attendre à une transmission imminente des données et qu'il y a péril en la demeure.

Même si la décision-modèle du Conseil fédéral est elle aussi assortie des sanctions de l'art. 292 CP, l'avantage des mesures provisionnelles ou superprovisionnelles réside dans le fait – sous réserve bien entendu d'une adjudication de ses conclusions – que ces sanctions pourront être directement imposées dans le cas concret.

L'avocat sera surtout confronté au défi majeur de suffisamment bien motiver sa requête, en particulier le *periculum in mora*, alors qu'il ne dispose que peu d'informations en raison du refus de la banque de lui fournir les informations auxquelles il aurait droit.

Pour conclure:

On l'a vu, la position de l'avocat est souvent délicate. Il est donc essentiel qu'il fasse usage, dès que possible, de tous les moyens qui sont à sa disposition pour s'opposer à une transmission des données.

Sources :

Liens :

Secrétariat d'Etat aux questions financières internationales (SFI) dans le différend fiscal avec les Etats-Unis :

http://www.sif.admin.ch/themen/00502/00806/index.html?lang=fr

Joint statement entre le DOJ et le DFF :

https://www.news.admin.ch/message/index.html?lang=fr&msg-id=50049

US program :

http://www.justice.gov/opa/pr/2013/August/13-tax-975.html

Demandes de renseignements :

http://www.edoeb.admin.ch/datenschutz/00628/00638/00640/index.html?lang=fr

Doctrine :

David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zurich 2008

Décisions judiciaires :

Tribunal supérieur de Zürich :

http://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/LB130059.pdf

Tribunal du district de Zürich :

http://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/CG120124-L.pdf