

US Program : le transfert de données clients pseudonymisées

Auteur : Emilie Jacot-Guillarmod

Date : 5 octobre 2018

[TF, 26.02.2018, 4A_365/2017](#)

Les données pseudonymisées de façon à empêcher l'identification de la personne concernée ne constituent pas des données personnelles. Cela étant, il incombe à l'auteur de la pseudonymisation de prouver que l'identification est effectivement rendue impossible.

Faits

Dans le cadre du [Joint Statement](#) de 2013 destiné à mettre un terme au contentieux fiscal américain impliquant des banques suisses, une banque décide de participer au **programme américain** avec l'autorité fiscale américaine et le Département fédéral de la justice des États-Unis (DoJ) dans la catégorie 2, ce qui signifie qu'elle estime avoir violé le droit américain. Les banques de catégorie 2 sont notamment tenues de **communiquer au DoJ diverses données** relatives à tout compte lié aux États-Unis et clos pendant la période visée par le programme (*Closed US Related Account*), notamment le nom du *relationship manager* concerné, certaines informations concernant le trafic de paiements, ainsi que la nature de la relation entre le compte et la personne américaine (p. ex. qualité de cliente ou d'ayant droit économique de cette dernière) (**liste II.D.2**).

La liste II.D.2 ne contient en revanche **aucune information permettant d'identifier directement le client**, les données telles que le nom du client et le numéro de compte étant remplacées par des **pseudonymes**. La banque conserve une **table de concordance** lui permettant de retrouver les vraies coordonnées du client.

Le Département fédéral des finances autorise la banque à fournir les informations visées par la liste II.D.2 ([art. 271 CP](#)). La banque signe ultérieurement un *Non-Prosecution Agreement (NPA)* avec le DoJ. Cet accord reprend les termes du *Joint Statement*. Il impose notamment à la banque de continuer à fournir les données visées par la liste II.D.2 après la signature du NPA.

Le titulaire et l'ayant droit économique d'un *Closed US Related Account* agissent en justice pour faire **interdire la transmission de la liste II.D.2**. Ils font valoir que les données contenues dans la liste II.D.2 **permettent indirectement de les identifier** et constituent dès lors des **données personnelles** au sens de la [LPD](#). Le *Handelsgericht* zurichois fait droit à leur demande ([arrêt du *Handelgericht* zurichois HG150-170 O du 30 mai 2017](#)).

Sur recours de la banque, le Tribunal fédéral doit déterminer **si les données visées par la liste II.D.2 constituent des données personnelles au sens de la LPD**, notamment au regard des mesures de **pseudonymisation** prises par la banque.

Droit

Le titulaire et l'ayant droit économique du compte font valoir que la transmission de la liste II.D.2 violerait leur droit à la **protection de leurs données personnelles** ainsi que les obligations contractuelles de la banque, en particulier son **devoir de confidentialité**.

Aux termes de l'[art. 3 let. a LPD](#), toutes les informations qui se rapportent à une personne

identifiée ou identifiable constituent des **données personnelles**. Une personne est identifiable lorsqu'il est possible de déduire son identité par recoupement d'informations. La banque fait valoir qu'au regard des mesures de pseudonymisation prises, les informations contenues dans la liste II.D.2 ne permettent pas au DoJ d'identifier le titulaire et l'ayant droit économique du compte et ne constituent de ce fait pas des données personnelles du point de vue du DoJ.

La **pseudonymisation** permet d'**échapper au champ d'application de la LPD** lors du transfert de données, **si elle empêche effectivement l'identification de la personne concernée par le récipiendaire des informations**. Toute possibilité théorique d'identifier la personne concernée ne suffit pas. On considérera que la personne est non-identifiable si les efforts nécessaires à son identification sont tels que selon l'expérience générale de la vie, leur mise en œuvre par le récipiendaire des informations est improbable. Dans ce contexte, on prend notamment en considération l'intérêt du récipiendaire à l'identification de la personne concernée.

Selon le *Handelsgericht*, la banque n'a pas **prouvé** l'impossibilité de l'identification par le DoJ. La banque conteste cette **répartition du fardeau de la preuve**. Elle fait valoir que l'existence de données personnelles constitue le fondement de la demande du client et de l'ayant droit économique, ce pourquoi les demandeurs devraient supporter le fardeau de la preuve correspondante ([art. 8 CC](#)).

Les informations contenues dans la liste II.D.2 **dérivent** indubitablement de **données personnelles**, notamment le nom du client. Lors du processus de pseudonymisation, la banque traite des données personnelles. La banque entend remettre le résultat de ce traitement au DoJ. Selon la banque, la transmission de la liste II.D.2 échappe au champ d'application de la LPD parce que les mesures de pseudonymisation prises **empêchent l'identification** des personnes concernées par le DoJ. Ce faisant, la banque fait valoir une **exception**. L'instance précédente a dès lors considéré à bon droit qu'**il incombait à la banque de prouver l'impossibilité de l'identification** par le DoJ.

Parmi les **mesures de pseudonymisation** prises, la banque a notamment additionné les paiements mensuels et indiqué dans la liste II.D.2 uniquement le montant mensuel global (**agrégation de données**). Ce procédé paraît propre à empêcher ou rendre plus difficile l'identification des ayants droit du compte. Contrairement à ce qu'a retenu l'instance précédente, le simple fait que le DoJ ait connaissance de cette mesure ne la rend pas inopérante. Par ailleurs, le remplacement d'identifiants (tels que le nom du client et le numéro de compte) par des **alias**, seule la banque ayant accès à la table de concordance, constitue a priori une mesure de pseudonymisation appropriée. Cela étant, le *Handelsgericht* relève que **le nom du relationship manager est communiqué en clair** dans la liste II.D.2. Selon l'instance précédente, ceci constituerait un **point d'ancrage** permettant au DoJ d'en apprendre plus sur le compte, et ultimement de déduire de l'ensemble des informations transmises l'identité du titulaire et de l'ayant droit économique. La banque **ne motive pas suffisamment** en quoi ce raisonnement viole le droit ([art. 42 al. 2 LTF](#)). Sur la base des considérations de l'instance précédente, insuffisamment contestées, il sied dès lors d'admettre que **le titulaire et l'ayant droit économique du compte sont identifiables sur la base de l'ensemble des informations** comprises dans la liste II.D.2.

Selon l'arrêt contesté, la banque est **contractuellement** tenue à la **confidentialité** uniquement dans la mesure où les informations concernées permettent d'identifier le client. Ce point n'est plus litigieux devant le Tribunal fédéral. Partant, le raisonnement qui précède permet également de déterminer le champ d'application du devoir contractuel de confidentialité de la banque.

Au regard de ce qui précède, **les données contenues dans la liste II.D.2 constituent des données personnelles au sens de la LPD** et des données soumises au devoir de confidentialité contractuel. Le *Handelsgericht* a dès lors interdit la transmission de la liste II.D.2 à bon droit.

Partant, le Tribunal fédéral rejette le recours.

Note

La littérature distingue l'anonymisation de la pseudonymisation. L'**anonymisation** empêche définitivement le rattachement des données à une personne précise, y compris par l'auteur du traitement. Par opposition, la **pseudonymisation** est un procédé par lequel on substitue aux éléments permettant une identification directe un identifiant neutre. L'auteur du traitement conserve une table de concordance permettant de rattacher les données pseudonymisées à la personne concernée.

Cet arrêt apporte une clarification bienvenue quant à **la qualification juridique des données pseudonymisées**. En effet, en cas de transfert de données, la question de savoir **de quel point de vue** il convient d'apprécier la possibilité d'identifier la personne concernée est controversée. Selon certains auteurs, il suffit que **soit l'exportateur des données, soit le récipiendaire** puisse identifier la personne à laquelle se rapportent les données pour que ces données constituent des données personnelles pour les deux parties au transfert (approche dite "**alternative**"). Selon cette approche, **les données pseudonymisées constitueraient en tout état des données personnelles**, puisque l'exportateur de données peut retrouver la personne concernée au moyen de la table de concordance. À noter que les auteurs en faveur de cette approche se réfèrent notamment à l'arrêt dit "Logistep" ([ATF 136 II 508](#)), dont la portée est débattue en doctrine.

Par opposition, d'autres auteurs retiennent que **la possibilité d'identifier la personne concernée s'apprécie de façon relative, selon le point de vue de l'intéressé** (approche dite "**relative**"). Des données pseudonymisées pourraient ainsi constituer des données personnelles du point de vue de l'exportateur (qui détient la table de concordance) et non de celui du récipiendaire (sous réserve de la possibilité pour celui-ci d'opérer des recoupements avec des données en clair).

Dans le contexte du **US Program**, la plupart des banques ont à notre connaissance adopté le procédé litigieux *in casu*. Elles ont ainsi transmis des données pseudonymisées au DoJ et conservé une table de concordance, afin de pouvoir réidentifier la personne concernée si des demandes ultérieures d'entraide en matière fiscale des autorités américaines devaient aboutir. Le **Préposé fédéral a critiqué** cette façon de procéder dans [une prise de position de 2014](#), considérant que les données pseudonymisées constituaient en toute hypothèse des données personnelles, selon l'approche "alternative" susvisée.

L'arrêt résumé ici valide dans le cas d'espèce **l'approche dite "relative"** de la qualification des données personnelles. Cette approche permet a priori des exportations facilitées de données pseudonymisées. Ceci est toutefois relativisé par le fait que le Tribunal fédéral **fait peser sur l'exportateur** le fardeau de la preuve de l'impossibilité d'identification par le récipiendaire. La preuve correspondante s'avérera fréquemment difficile à apporter. L'[arrêt cantonal](#) mentionne d'ailleurs expressément qu'il n'existe que peu de place pour une telle preuve au regard des possibilités techniques actuelles. Par ailleurs, au regard de la jurisprudence existante, notamment l'arrêt Logistep, on ne peut exclure que les tribunaux suivent l'approche alternative, plus restrictive, si ceci semble justifié au regard des circonstances concrètes.

En tout état, les exportateurs de données seront bien avisés de **documenter soigneusement les mesures de pseudonymisation** mises en place et les tests opérés pour s'assurer de l'impossibilité d'identification par le récipiendaire. Nous relevons que la preuve sera particulièrement difficile à apporter en cas de transfert de données à une autorité, au regard des moyens étendus d'obtenir des informations d'autres sources et d'opérer des recoupements dont disposera fréquemment cette dernière. A titre d'exemple, l'[arrêt cantonal](#) mentionne que les autorités américaines pourraient potentiellement avoir accès aux données des centres de

LawInside.

Swiss Case Law

<https://www.lawinside.ch>

traitement des paiements SWIFT situés aux États-Unis.

L'auteur du présent résumé travaille pour l'Étude qui a représenté la banque *in casu*.