Les données bancaires pseudonymisées – Du secret bancaire à la protection des données

Célian Hirsch | Emilie Jacot-Guillarmod*

Law strictly restricts the transfer of personal data and data protected by banking secrecy, especially outside of Switzerland. Personal data is defined as all information relating to an identified or identifiable person. Similarly, legal scholarship and case law hold that banking secrecy protects only client identifying data. The ability to identify the relevant person is thus core to both data protection and banking secrecy.

In practice, Swiss banks regularly share anonymized or pseudonymized data with third parties, including third parties located abroad. In this contribution, the authors discuss the circumstances in which the data subject is considered «identifiable», i.e. in which client data is protected by banking secrecy and the Swiss Federal Data Protection Act. Furthermore they analyze the implications for pseudonymized client data.

Table des matières

Introduction

La problématique de la pseudonymisation et de l'anonymisation des données bancaires n'est pas nouvelle, mais elle est récemment revenue sur le devant de la scène avec la publication du Guide « Cloud » de mars 2019 par l'Association suisse des banquiers (ASB)[1]. Selon cette association, l'anonymisation, la pseudonymisation et le cryptage permettent d'assurer le respect du secret bancaire et des règles en matière de protection des données lorsque des « données d'identification du client » (*client identifying data,* CID) sont sauvegardées sur un serveur *cloud* à l'étranger. En pratique, les banques recourent fréquemment à l'anonymisation ou à la pseudonymisation afin de limiter les risques liés à l'externalisation du traitement de données clients.

Néanmoins, les conséquences juridiques qui découlent de la pseudonymisation et de l'anonymisation et la répartition du fardeau de la preuve en la matière en cas de litige sont loin d'être claires. Une banque en a récemment fait l'amère expérience lors d'une action intentée par un client qui s'est opposé avec succès à la transmission à l'étranger de ses données prétendument pseudonymisées[2].

Dans la présente contribution, nous nous attelons à répondre aux questions suivantes : les données

* *Célian Hirsch* est avocat et doctorant au Centre de droit bancaire et financier de l'Université de Genève. *Emilie Jacot-Guillarmod* est avocate et MBA Candidate (INSEAD). Nous exprimons toute notre gratitude à Dr *Yaniv Benhamou* et Me *Jeremy Bacharach* pour leur relecture attentive et leurs commentaires pertinents.

1 Guide « Cloud » de mars 219 publié par l'Association suisse des banquiers (ASB) ; cf. également les deux avis de droit mandatés par l'ASB et publiés dans la Jusletter du 27 mai 2019 (*Laux Christian/Hofmann Alexander/Schieweck Mark/Hess Jürg,* Nutzung von Cloud-Angeboten durch Banken, Jusletter du 27 mai 2019 ; *Isler Michael/Kunz Oliver M./Müller Thomas/Schneider Jürg/Vasella David,* Bekanntgabe von Bankkundendaten an Beauftragte im In- und im Ausland, Jusletter du 27 mai 2019).

2 Arrêt du *Handelsgericht* zurichois HG150170-O du 30 mai 2017 confirmé par l'arrêt du Tribunal fédéral 4A_365/2017 du 5 octobre 2018, résumé par *Jacot-Guillarmod Emilie,* US Program : le transfert de données clients pseudonymisées, <*www.LawInside.ch/660/*> (tous les liens hypertextes contenus dans la présente contribution ont été consultés pour la dernière fois le 10 février 2020).

bancaires pseudonymisées sont-elles soumises au secret bancaire, respectivement à la Loi sur la protection des données ? Le champ d'application de ces deux régimes de protection est-il identique ? Par ailleurs, en cas de procédure judiciaire en lien avec le traitement de données pseudonymisées ou anonymisées, appartient-il à la banque ou au client de démontrer l'anonymisation ou la pseudonymisation ?

Premièrement, nous examinons la portée de la pseudonymisation sous l'angle du secret bancaire (section I). Afin de situer la discussion, nous rappelons les sources du secret bancaire (section I.1) et prenons position sur son étendue, notamment sous l'angle du *cloud banking* (section I.2). Nous abordons ensuite la possibilité de transmettre des données bancaires en clair sur la base du consentement contractuel, avant d'analyser la question de la pseudonymisation et de l'anonymisation (section I.3).

Deuxièmement, nous analysons les conséquences juridiques de la pseudonymisation au regard de la Loi sur la protection des données (section II). Nous rappelons quelles données constituent des données personnelles au sens de cette loi (section II.1). Nous examinons ensuite si les données bancaires anonymisées (section II.2) et pseudonymisées (section II.3) doivent être qualifiées de données personnelles au sens de cette définition.

Troisièmement, nous nous penchons sur la répartition du fardeau de la preuve en la matière (section III). En effet, sous l'angle de la gestion des risques, il est important pour la banque de comprendre le fardeau de preuve qu'elle supporte si son client devait agir en justice contre le traitement de ses données anonymisées ou pseudonymisées. Dans ce contexte, nous rappelons que la répartition du fardeau de la preuve est différente pour les faits générateurs de droits et les faits dirimants (section III.1). À la lumière de ce principe, nous analysons ensuite à quelle partie il incombe de prouver l'anonymisation, respectivement la pseudonymisation (section III.2).

Dans un dernier temps, nous présentons quelques suggestions pour la pratique bancaire au regard des développements juridiques présentés (section IV).

I. Secret bancaire

1. Source du secret

Le secret bancaire trouve son fondement dans deux sources juridiques distinctes[3] :

- La protection de la personnalité (art. 28 CC)[4] ;
- Le devoir de diligence et de fidélité du mandataire (art. 398 al. 2 CO)[5] et, pour les contrats bancaires auxquels les règles du mandat ne sont pas applicables, le principe général de la bonne foi (art. 2 al. 1 CC)[6].

L'art. 47 LB, incriminant pénalement la violation du secret bancaire qui est parfois également mentionné comme fondement du secret bancaire[7], ne fait en réalité que reprendre l'obligation de droit privé de traiter de manière confidentielle les informations du client en rendant punissable, pour certaines personnes, la violation de ce devoir[8]. Cette norme est néanmoins pertinente pour vérifier quelles personnes sont assujetties au secret, comme nous allons le voir ci-dessous.

3 ATF 145 IV 114, c. 3.3.2 *Aubert Maurice et al.,* Le secret bancaire suisse, 3e éd.,Berne 1995, p. 52 ss ; BSK BankG-*Stratenwerth,* art. 47 LB N 1 ; *Lombardini Carlo,* Droit bancaire suisse, 2e éd., Zurich/Bâle/Genève 2008, p. 965 s ; le secret bancaire est également protégé par la Constitution (art. 13 Cst.), bien qu'il n'ait pas le statut de droit fondamental (*Biaggini Giovanni,* art. 13 Cst. N 1*a*, in : BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2e éd., Zurich 2017).

4 L'art. 28 CC dispose que celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe ; le secret bancaire trouve ainsi son origine notamment dans la même source que la protection des données : la protection du droit à la personnalité.

5 Aux termes de l'art. 398 al. 2 CO, le mandataire est responsable envers le mandant de la bonne et fidèle exécution du mandat.

6 L'art. 2 al. 1 CC prévoit que chacun est tenu d'exercer ses droits et d'exécuter ses obligations selon les règles de la bonne foi.

7 *Lombardini* (n. 3), p. 965 s.

8 ATF 145 IV 114, c. 3.3.2 ; ATF 142 III 116, c. 3.1.2 ; arrêt du Tribunal fédéral 4A_522/2018 du 18 juillet 2019, c. 4.5.2 ; l'art. 47 LB ne constitue donc pas une base légale propre au secret bancaire (*Winkler Markus,* Grenzbetrachtungen zum Bankgeheimnis, Jusletter du 3 juin 2019, N 1).

2. Étendue du secret et cloud banking

Le secret bancaire désigne l'obligation à la charge de tout organe, employé, mandataire ou liquidateur d'une banque (les détenteurs du secret) de garder confidentielles toutes les informations qui leur sont données par le client dans le cadre de la relation commerciale ou qui sont portées à leur connaissance dans ce contexte[9]. Est protégé par le secret bancaire l'existence même du rapport contractuel avec une banque, les connaissances issues d'une relation d'affaires entre la banque et le client, notamment les contrats bancaires, mais également toutes les requêtes et offres de relations bancaires ainsi que toutes les transactions et les opérations que la banque fait avec ses clients, qu'elles soient ou non de nature bancaire[10].

Le maître du secret est en principe le client. Cela étant, l'ayant droit économique peut également se prévaloir du secret bancaire s'il est au bénéfice d'une stipulation pour autrui parfaite[11]. De plus, dans la situation où la relation contractuelle passe aux héritiers, et qu'ils deviennent ainsi maîtres du secret, le défunt bénéficie encore de son droit à la protection de la personnalité, lequel doit être pris en compte par la banque[12].

Dans le cadre du *cloud banking,* se pose la question de savoir si le prestataire de services *cloud*[13] est également soumis au secret bancaire ou s'il est considéré comme un tiers auxquels les banques ne peuvent pas transmettre des données bancaires sans violer leur secret. Concrètement, cela revient à devoir déterminer si ce prestataire est un « mandataire » au sens de l'art. 47 LB, et donc soumis au secret, ou s'il est un tiers, auquel cas le secret ne peut pas lui être révélé.

Bien que le Tribunal fédéral ne se soit pas (encore) prononcé sur cette question, il a récemment affirmé, au sujet de l'exploitation d'un espace de coworking pour avocats, que « le professionnel externe chargé de la conservation et de la protection à distance des données informatiques » est un auxiliaire de l'avocat[14] au sens de l'art. 101 CO et donc soumis au secret professionnel[15]. A noter néanmoins que la notion de mandataire au sens de l'art. 47 LB doit être interprétée restrictivement[16], alors que la notion d'auxiliaire au sens de l'art. 101 CO est large[17].

Les deux avis de droit mandatés par l'ASB sont arrivés à la conclusion, après un examen détaillé, que le prestataire de services *cloud* est un mandataire au sens de l'art. 47 LB et donc également soumis au secret bancaire[18]. Selon nous, une telle conclusion est particulièrement convaincante au regard de l'interprétation historique de cette norme. En effet, lors de la révision de la Loi sur les banques de 1971, le Conseil fédéral a proposé au Parlement d'ajouter les « mandataires » de banque *(die Beauftragte)* aux personnes soumises au secret en vertu de l'art. 47 LB afin d'y inclure « en particulier les centres de calcul qui sont chargés par les banques du traitement électronique des informations »[19]. La doctrine majoritaire soutient également que le prestataire de services externalisés doit être qualifié de mandataire au sens de l'art. 47 LB[20].

9 ATF 145 IV 114, c. 3.3.2 ; cf. également ATF 137 II 431, c. 2.1 ; *Aubert et al.* (n. 3), p. 43.

10 HG150170 (n. 2), c. 5.3.4.2 ; Bulletin FINMA 4/2013, p. 73 s ; *Lombardini* (n. 3), p. 967 s.

11 HG150170 (n. 2), c. 5.3.9.2 ; cf. également BK-*Fellmann,* art. 398 CO N 69.

12 Arrêt du Tribunal fédéral 4A_522/2018 du 18 juillet 2019, c. 4.5.2.

13 Le terme *cloud* utilisé ici comprend les trois principaux types de services proposés, à savoir le SaaS *(Software as a Service),* le PaaS *(Platform as a Service)* et le IaaS *(Infrastructure as a Service)*.

14 De nombreux auteurs s'étaient prononcés sur la question du cloud en relation avec le secret de l'avocat : *Chappuis Benoît/Alberini Adrien,* Secret professionnel de l'avocat et solutions cloud, Revue de l'avocat 2017, p. 337 ss ; *Benhamou Yaniv/Erard Frédéric/Kraus Daniel,* L'avocat a-t-il aussi le droit d'être dans les nuages ?, Revue de l'avocat 2019, p. 119 ss ; *Schwarzenegger Christian/Thouvenin Florent/Stiller Burkhard/George Damian,* Utilisation des services de cloud par les avocats, Revue de l'avocat 2019, p. 33 ss ; *Wohlers Wolfgang,* Outsourcing durch Berufsgeheimnisträger, digma 2016, p. 114 ss ; *Wohlers Wolfgang,* Auslagerung einer Datenbearbeitung und Berufsgeheimnis, Rechtsgutachten im Auftrag des Datenschutzbeauftragten des Kantons Zürich, Zurich 2016.

15 ATF 145 II 229, c. 7.3.

16 ATF 145 IV 114, c. 3.3.4

17 ATF 145 II 229, c. 7.3.

18 *Laux/Hofmann/Schieweck/Hess* (n. 1) N 39 ; *Isler/Kunz/Müller/Schneider/Vasella* (n. 1), N 59.

19 Message du Conseil fédéral du 13 mai 1970 à l'Assemblée fédérale concernant la révision de la loi sur les banques, FF 1970 1197.

20 Cf. *Cassani Ursula/Villard Katia,* La responsabilité pénale pour l'infraction commise dans le cadre d'activités outsourcées, in : Jositsch Daniel/Schwarzenegger Christian/Wohlers Wolfgang (édit.), Festschrift für Andreas Donatsch, Zurich 2017, p. 590 et doctrine citée en note 33.

Cela étant, une telle conclusion ne permet pas, à notre avis, d'affirmer que la transmission de données protégées par le secret bancaire à un prestataire *cloud* étranger n'est pas pénale. En effet, bien que le prestataire étranger puisse être soumis au champ d'application personnel de l'art. 47 LB comme « mandataire », il n'en demeure pas moins qu'il ne tombe probablement plus dans le champ d'application territorial du droit pénal suisse (cf. art. 3–8 CP)[21].

Conformément aux développements qui précèdent, la transmission de données bancaires en clair à un prestataire de services en Suisse est en principe admissible sous l'angle du secret bancaire[22]. En revanche, une telle transmission à l'étranger semble, selon nous, problématique sous l'angle du secret bancaire.

Nous examinerons à présent si (section I.3.1) le consentement du client ou (section I.3.2) la pseudonymisation et l'anonymisation des données bancaires (deux cas de figure fréquents en pratique) permettent un tel transfert à l'étranger.

3. Deux limitations possibles

3.1 Consentement contractuel

Premièrement, il faut garder à l'esprit que le maître du secret bancaire est le client *(Bankkundengeheimnis)*. Il peut ainsi libérer la banque de son obligation de confidentialité[23]. Le consentement[24] à la levée du secret doit être libre[25] et éclairé[26]. Il peut être admis de manière tacite si l'attention du client a été attirée sur la clause de manière appropriée[27]. Le consentement ne requiert toutefois pas de forme particulière[28]. Il peut être donné a *posteriori*[29] et être retiré en tout temps[30].

En pratique, la renonciation, au moins partielle, au secret bancaire se trouve fréquemment dans des conditions générales qui sont soit directement approuvées par le client (intégration individuelle) soit auxquelles le contrat principal renvoie (intégration globale)[31]. La question de la validité de la renoncia-

21 La question de la punissabilité d'une violation du secret bancaire à l'étranger dépend de la qualification de cette infraction en tant que délit formel *(schlichtes Tätigkeitsdelikt)* ou de délit matériel *(Erfolgsdelikt)*. En tant que délit formel, la violation du secret bancaire à l'étranger ne serait pas punissable. Au contraire, en tant que délit matériel, le résultat pourrait se produire en suisse au sens de l'art. 8 CP (TPF, SK.2016.34 du 21 janvier 2019, c. 1.6.5.3). Alors que le Tribunal fédéral a expressément laissé cette question ouverte dans l'ATF 145 IV 144, c. 3.4. (arrêt dit « Rudolf Elmer », résumé, <*LawInside.ch/727*>), le Tribunal pénal fédéral considère que la violation du secret bancaire constitue un délit formel (TPF, SK.2016.34 du 21 janvier 2019, c. 1.6.5.4 ; *contra Isler/Kunz/Müller/Schneider/Vasella* [n. 1], N 45 et *Laux/Hofmann/Schieweck/Hess* [n. 1], N 18).

22 L'anonymisation ou la pseudonymisation constituent en tout état de bonnes pratiques permettant de limiter les risques opérationnels liés à l'externalisation et d'assurer le respect du principe *need-to-know,* cf. FINMA, Circulaire 2008/21, Annexe 3, Cm. 15.

23 *Lombardini* (n. 3), p. 970 ; *von Burg Johanna,* L'exécution fidèle : le devoir de discrétion/le secret bancaire du négociant, in : Bizzozero Alessandro/Falletti André/Meregalli Do Duc Samantha (édit.), Le mandat de gestion de fortune, Zurich 2017, p. 308 ; *Rappo Aurélia,* Les fondements juridiques actuels du secret bancaire, in : Augsburger-Bucheli Isabelle/Perrin Bertrand (édit.), Les enjeux du secret bancaire, Genève 2011, p. 46 ; BSK BankG-*Stratenwerth,* art. 47 LB N 25 ; *Margiotta Adriano,* Das Bankgeheimnis : Rechtliche Schranke eines bankkonzerninternen Informationsflusses ?, thèse Saint-Gall, Zurich 2002, p. 93.

24 A noter que la notion de « consentement » relève du droit privé et ne constitue dès lors ni un fait excluant la typicité prévue par l'art. 47 LB ni un fait justificatif au sens du droit pénal (*Aubert et al.* [n. 3], p. 106).

25 « Libre » signifie qu'il ne doit notamment pas être vicié, à savoir s'il a été donné sous l'emprise d'une erreur, d'un dol voire d'une crainte fondée (BSK BankG-*Stratenwerth,* art. 47 LB N 27).

26 « Éclairé » signifie que le client doit recevoir des informations suffisantes sur les conséquences essentielles de sa renonciation au secret (*Margiotta* [n. 23], p. 94).

27 *Rappo* (n. 23), p. 46 qui cite l'ATF 98 IV 217 relatif au secret professionnel protégé par l'art. 321 CP. Dans cet arrêt, le client a assisté *sans réagir* à la remise à la police d'un certificat contenant des informations confidentielles ; son attitude a ainsi été interprétée par le Tribunal fédéral comme un acquiescement (ATF 98 IV 217, c. 2).

28 *Margiotta* (n. 23), p. 94.

29 *Margiotta* (n. 23), p. 94.

30 *Margiotta* (n. 23), p. 95 qui se fonde sur l'art. 27 al. 2 CC (nul ne peut aliéner sa liberté, ni s'en interdire l'usage dans une mesure contraire aux lois ou aux mœurs) ; cf. également *Pedrazzini Mario M./Oberholzer Niklaus,* Grundriss des Personenrechts, 4e éd., Berne 1993, p. 125.

31 Une clause de conditions générales imprimée en gras stipulant qu'avec la signature des conditions générales le client donnait son accord quant à la levée partielle du secret bancaire dans la mesure où celle-ci était nécessaire pour permettre le traitement de données à l'étranger, a ainsi été jugée suffisante par la Commission Fédérale des Banques pour considérer que le client avait validement consenti à la levée du secret bancaire (Bulletin CFB, Fasci-

tion au secret bancaire doit alors également être examinée au regard de la règle de la théorie de la clause insolite[32] et de l'art. 8 LCD qui prohibe les conditions générales abusives[33]. De plus, une renonciation totale au secret bancaire pourrait se heurter à la nullité de l'engagement excessif prévue par l'art. 27 al. 2 CC[34]. Enfin, afin que le consentement soit valable, la clause devrait décrire aussi précisément que possible la finalité, le contenu et les personnes auxquelles les données soumises au secret peuvent être communiquées[35]. Il est intéressant de relever que ces exigences d'informations correspondent largement à celles du droit de la protection des données[36]. Si ces exigences sont respectées, le consentement du client constitue un motif justificatif valide permettant de communiquer des données bancaires à un tiers, y compris à l'étranger.

En pratique, l'obtention du consentement du client peut toutefois s'avérer difficile[37] ou indésirable du point de vue commercial[38]. Dans de telles circonstances, il est intéressant de déterminer si, alternativement, la banque peut soustraire les données au champ d'application du secret bancaire en les anonymisant ou les pseudonymisant[39].

3.2 Pseudonymisation et anonymisation

Comme nous le verrons plus en détail ci-dessous, la pseudonymisation et l'anonymisation permettent de restreindre, partiellement respectivement complètement, la possibilité d'identifier une personne à partir de données la concernant[40].

Il convient d'examiner, à l'aune de la jurisprudence, de la pratique de la FINMA et de la doctrine, si la pseudonymisation ou l'anonymisation de données bancaires a également pour effet de soustraire les données bancaires à la protection prévue par le secret bancaire. Tel est le cas si les données bancaires ne sont protégées qu'à la condition qu'elles se rapportent à une personne identifiée ou identifiable.

3.2.1 Jurisprudence

À notre connaissance, la jurisprudence fédérale ne s'est jamais expressément prononcée sur l'application du secret bancaire lorsque les données bancaires ne se rapportent pas à une personne identifiée ou identifiable.

Dans l'ATF 141 III 119, le Tribunal fédéral semble mettre l'accent, bien que très brièvement, sur le caractère de l'*identification* des clients afin que le secret

cule 21, p. 30). *Margiotta* estime toutefois que des circonstances particulières sont nécessaires pour accepter un consentement tacite (*Margiotta* [n. 23], p. 95 s.).

32 ATF 138 III 411, c. 3.1 ; CR CO I-*Morin,* art. 1 CO N 176 ss ; *Tercier Pierre/Pichonnaz Pascal,* Le droit des obligations, 6e éd., Genève/Zurich/Bâle 2019, N 948 ss.

33 L'art. 8 LCD prévoit qu'agit de façon déloyale celui qui, notamment, utilise des conditions générales qui, en contradiction avec les règles de la bonne foi prévoient, au détriment du consommateur, une disproportion notable et injustifiée entre les droits et les obligations découlant du contrat. A ce sujet, cf. notamment *Bahar Rashid,* Conditions générales : a time for change, in : Thévenoz Luc/Bovet Christian (édit.), Journée 2011 de droit bancaire et financier, Genève 2012, p. 131 ss.

34 *Margiotta* (n. 23), p. 100 qui compare cette renonciation totale à la cession de créance portant sur toutes les créances futures d'une personne, laquelle est contraire à l'art. 27 al. 2 CC.

35 *Margiotta* (n. 23), p. 99 s. ; la Commission Fédérale des Banques a reconnu la validité d'une renonciation au secret bancaire dans des conditions générales qui prévoyaient expressément et en caractères gras la levée du secret pour le traitement des données au Royaume-Uni (Bulletin CFB, Fascicule 21, p. 30).

36 Art. 4 al. 5 et art. 14 al. 2 LPD ; art. 5 al. 6 et art. 17 P-LPD.

37 Par exemple, dans le cadre du *US Program for Swiss Banks* (*Joint Statement between the US Department of Justice and the Swiss Federal Department of Finance,* 29 août 2013), les banques n'ont pas cherché à obtenir un consentement *ad hoc* à la transmission de certaines informations relatives à leurs clients américains au Département de Justice, un tel exercice apparaissant largement voué à l'échec et en tout état impracticable dans les délais utiles. Elles sont donc reposées d'une part sur les clauses contractuelles préexistantes et d'autre part sur la prétendue pseudonymisation des données transmises (cf. p. ex. HG150170 [n. 2]).

38 Satisfaire au devoir d'information décrit ci-dessus peut par exemple s'avérer délicat si les clients perçoivent la communication à l'étranger comme une atteinte à la confidentialité souhaitées dans leur relation d'affaire avec un banque suisse.

39 Précisons que même si le prestataire est un « mandataire » au sens de l'art. 47 LB, la banque demeure tenue par la LPD d'informer ses clients des catégories de destinataires auxquelles leurs données personnelles sont transmises (art. 4 al. 5 et art. 14 al. 2 LPD ; art. 5 al. 6 et art. 17 P-LPD). Par opposition, une solution qui soustrairait les données tant au champ d'application du secret bancaire qu'à celui de la LPD rendrait ce devoir d'information inapplicable. Selon les développements qui suivent, l'anonymisation et la pseudonymisation pourraient constituer de telles solutions.

40 Cf. *infra* sections II.2 et II.3.

bancaire protégé s'applique[41]. De son côté, le Tribunal pénal fédéral semble avoir la même approche : seules les informations permettant l'identification des clients des banques suisses – qu'elles soient détenues par la banque, un avocat ou un mandataire – sont protégées par l'ordre public suisse[42]. Il semble ainsi que, *a contrario,* une information ne permettant pas d'identifier un client ne soit pas protégée par le secret bancaire.

Récemment, le *Handelsgericht* zurichois a considéré que des données bancaires pseudonymisées ou anonymisées de manière efficace ne sont plus protégées par le secret bancaire[43]. Concrètement, ce tribunal a dû examiner si des données clients, prétendument pseudonymisées, pouvaient être transmises au *Department of Justice* (DoJ) dans le cadre du programme américain[44]. En l'espèce, il a retenu que la pseudonymisation n'était pas efficace puisque le DoJ pouvait, à l'aide d'efforts raisonnables, réidentifier les personnes concernées par les données bancaires.

3.2.2 FINMA

Dans sa Circulaire 2008/21 sur les risques opérationnels, la FINMA dispose que les banques doivent prévoir un cadre adéquat garantissant la confidentialité des « données d'identification du client » (*client identifying data,* CID)[45]. Ces données comprennent les données d'identification directe des clients[46], les données d'identification indirectes des clients[47] et les données d'identification potentiellement indirectes des clients[48]. Le critère essentiel repose donc sur l'*identification* du client. Ainsi, et *a contrario,* la divulgation d'une information ne permettant pas d'identifier un client ne présente pas un risque opérationnel au regard de la FINMA[49].

De manière plus concrète, la FINMA s'est prononcée sur l'importance de l'identification des clients dans un cas de vol de données bancaires dans le cadre d'une procédure d'*enforcement*. Elle a ainsi pu souligner qu'est déterminante la possibilité, pour le voleur de données bancaires, d'établir le lien entre des données patrimoniales qui ne sont pas attribuées à un client déterminé et les données d'identification des

41 ATF 141 III 119, c. 5.3 ; cet ATF traite du droit d'accès des employés d'une banque aux données les concernant qui ont été transmises aux autorités américaines. La banque a alors invoqué l'art. 47 LB comme motif justifiant le refus à l'accès aux documents requis puisque ceux-ci permettraient d'identifier les clients (pour un résumé de l'ATF 141 III 119, cf. *Schürch Simone,* Les données d'employés d'une banque transmises aux autorités américaines, <*www.LawInside.ch/14/*>).

42 Arrêt du Tribunal pénal fédéral SK.2017.64 du 9 mai 2018, c. 4.2.7 ; pour un commentaire de cet arrêt, cf. *Villard Katia,* Transmission de données clients aux USA : Guilty or not guilty ?, publié le 5 Septembre 2018 par le Centre de droit bancaire et financier, <*https://www.cdbf.ch/1022/*> ; *Hirsch Célian,* La transmission directe d'informations concernant des clients au Gouvernement américain (271 CP), <*www.lawinside.ch/646/*>.

43 HG150170 (n. 2), c. 5.3.5.5 ; à noter que le *Handelsgericht* se réfère uniquement à la doctrine relative à la protection des données, et non au droit bancaire, lorsqu'il examine si les données bancaires en cause ont été pseudonymisées de manière efficace.

44 HG150170 (n. 2), c. 5.3.5.1 ; pour les autres récents arrêts relatifs à la transmission de données bancaires dans le cadre du programme américain, cf. TF 4A_522/2017 du 10 avril 2018 ; 4A_514/2017 du 10 avril 2018 ; 4A_516/2017 du 10 avril 2018 ; 4A_324/2017 du 16 avril 2018 ; 4A_174/2018 du 22 août 2018 ; 4A_280/2018 du 24 août 2018 ; 4A_478/2018 du 9 octobre 2018 ; 4A_469/2018 du 12 octobre 2018 ; 4A_493/2018 du 15 octobre 2018 (cf. *Emmenegger Susan/Thévenoz Luc/Reber Martina/Hirsch Célian,* Das schweizerische Bankprivatrecht 2018/Le droit bancaire privé suisse 2018, RSDA 2019, p. 190 ss, r43). Précisons que la licéité du transfert de données client pseudonymisées dans le cadre du programme américain avait été contestée devant le Tribunal administratif en lien avec une requête d'assistance administrative en matière fiscale. Le Tribunal administratif fédéral avait toutefois retenu que la licéité dudit transfert n'était pas déterminante pour l'issue de la cause (A-4695/2015 du 2 mars 2015, c. 6.7.2 ss ; cf. également à ce sujet l'arrêt du TF 2C_1042/2016 du 12 juin 2018 qui souligne l'importance du *Joint Statement* pour le transfert de données bancaires aux Etats-Unis).

45 La FINMA précise que la pseudonymisation et l'anonymisation constitue précisément des mesures techniques garantissant la confidentialité (FINMA, Circulaire 2008/21, Cm 12).

46 P. ex. prénom, deuxième nom, nom de famille.

47 P. ex. numéro de passeport.

48 P. ex. combinaison de la date de naissance, de la profession, de la nationalité, etc.

49 La FINMA indique précisément que lorsque les CID sont stockées hors de Suisse ou qu'elles font l'objet d'un accès depuis l'étranger, elles « doivent être protégées de manière adéquate (p. ex. anonymisation, chiffrement ou pseudonymisation) » (FINMA, Circulaire 2008/21, Annexe 3, Cm 21). Elle précise expressément que les données anonymisées « ne sont/contiennent plus des CID et ne sont pas soumises à la LPD » (FINMA, Circulaire 2008/21, Annexe 3, Cm 65) ; cf. également *Fischer Philipp,* L'externalisation de services dans le domaine bancaire et financier, RSDA 2016, p. 137 ss.

clients[50]. Des données patrimoniales, qui ne permettent pas d'identifier les personnes auxquelles elles se rapportent, ne sont ainsi protégées par le secret bancaire qu'à la condition qu'elles puissent être couplées à des données d'*identification* client[51].

3.2.3 Doctrine

À notre connaissance, et jusqu'à très récemment, la doctrine relative au secret bancaire ne s'était pas penchée sur la question de savoir si la pseudonymisation ou l'anonymisation a pour conséquence de soustraire une information de la protection originellement prévue par le secret bancaire[52]. Désormais, la récente doctrine s'appuie précisément sur le récent arrêt du *Handelsgericht* susmentionné[53] afin d'affirmer que l'art. 47 LB ne s'applique pas aux informations anonymes[54].

La doctrine relative au secret professionnel considère que l'art. 321 CP est violé uniquement si la révélation permet au récipiendaire de « suffisamment identifier le secret et son maître »[55]. Ainsi, si le contenu protégé par le secret est « anonymisé », il peut être dévoilé à des tiers sans pour autant constituer une violation de l'art. 321 CP[56].

3.2.4 Notre analyse

Selon nous, l'interprétation téléologique du secret bancaire est en l'espèce déterminante. Rappelons-nous que cette interprétation nous amène à rechercher le but de la règle, son esprit, ainsi que les valeurs sur lesquelles elle repose, singulièrement l'intérêt protégé[57]. Or le secret bancaire a pour but de protéger la personnalité du client[58]. Dès lors que des données bancaires ne permettent plus d'identifier le client, sa personnalité n'a plus à être protégée en limitant la transmission ou la révélation de ses données. Ainsi, selon l'interprétation téléologique, le secret bancaire ne s'applique pas aux données bancaires pseudonymisées ou anonymisées.

Une approche systématique, laquelle a pour but de déterminer sa relation avec d'autres dispositions légales, confirme l'interprétation téléologique. Le secret bancaire trouve notamment son origine dans la même source que le droit de la protection des données[59] : la protection de la personnalité (art. 28 CC). Or, comme nous allons le voir ci-dessous[60], le droit de la protection des données ne s'applique plus dès que la personne concernée par les données n'est plus identifiable. Une approche cohérente du droit de la protection de la personnalité revient à préconiser la même solution pour le secret bancaire.

Bien qu'elles n'apportent pas de clarification supplémentaire à l'égard de notre problématique les interprétations historique et littérale ne s'opposent pas à la solution retenue ici. En effet, ni le Message du Conseil fédéral concernant le projet de la LB du 2 février 1934[61] ni les débats parlementaires[62] ne contiennent une quelconque indication relative au secret bancaire. S'agissant du texte légal, bien que le terme allemand *Bankkundengeheimnis* souligne le lien entre le secret et le client, la terminologie *Bankgeheimnis* est plus utilisée. Or une interprétation littérale du terme « secret bancaire/*Bankgeheimnis* » ne nous est d'aucune utilité pour résoudre la problématique.

Partant, en raison de l'interprétation téléologique et systématique, nous considérons que les don-

50 « A cela s'ajoute que le voleur présumé a également soustrait au moins (…) données de positions financières de clients et est parvenu à établir le lien entre les données d'identification des clients et ces données patrimoniales. Ces données, une fois couplées aux données d'identification des clients, sont également soumises au secret bancaire puisqu'elles permettent à un tiers de connaître la situation patrimoniale du client au sein de la banque et même dans certains cas d'établir un profil client » (Bulletin FINMA 4/2013, p. 76).

51 Bulletin FINMA 4/2013, p. 76

52 Ni *Stratenwerth* (n. 3) ni *Lombardini* (n. 3) ni *Aubert et al.* (n. 3) ni *Margiotta* (cf. n. 23) ne mentionnent cette problématique. *Kleiner/Schwob/Winzeler* évoquent certes l'anonymisation des données clients, mais uniquement de manière brève et dans le contexte particulier des publications de travaux de recherche historiques (*Kleiner/Schwob/Winzeler,* Kommentar zum BankG, art. 47 LB N 354 s.)

53 Cf. *supra* n. 2.

54 *Isler/Kunz/Müller/Schneider/Vasella* (n. 1) affirment précisément que l'art. 47 LB ne s'applique pas aux informations anonymes en se référant exclusivement à l'arrêt du *Handelsgericht* (N 30).

55 CR CP II-*Chappuis,* art. 321 CP N 71 ; *Corboz Bernard,* Les infractions en droit suisse, vol. 2, 3e éd., Berne 2010, art. 321 CP N 69.

56 CR CP II-*Chappuis,* art. 321 CP N 71 ; StGB PK-*Trechsel/Vest,* art. 321 CP N 23.

57 TF 4A_328/2019 du 9 décembre 2019, c. 3.2.2.

58 Cf. *supra* section I.1.

59 Cf. art. 1 LPD.

60 Cf. *infra* section II.

61 FF 1934 I 172, p. 189.

62 *Tobler Stefan,* Der Kampf um das Schweizer Bankgeheimnis, Eine 100-jährige Geschichte von Kritik und Verteidigung, Zurich 2019, p. 52.

nées bancaires pseudonymisées ou anonymisées ne sont pas protégées par le secret bancaire.

Cette solution a l'avantage d'être consistante avec la jurisprudence et en particulier avec l'arrêt du *Handelsgericht*. Elle est également cohérente avec la doctrine, certes relativement lapidaire, relative à l'art. 321 CP [63]. En outre, elle semble correspondre à la pratique[64].

Néanmoins, ni la doctrine ni la jurisprudence en droit bancaire ne précisent ce qu'il faut comprendre par « données pseudonymisées » et par « données anonymisées ». Pour mieux saisir ces notions, nous suggérons d'examiner la jurisprudence et la doctrine relatives au droit de la protection des données, laquelle s'est précisément penchée sur ces deux notions depuis de nombreuses années.

II. LPD : la notion de données personnelles

1. Définition légale

À teneur de l'art. 3 let. a LPD, sont des données personnelles au sens de la LPD « toutes les informations qui se rapportent à une personne identifiée ou identifiable ». La possibilité d'identifier la personne concernée constitue ainsi l'une des pierres angulaires du champ d'application matériel de la LPD : à défaut de possibilité d'identification, la LPD ne s'applique pas.

Une personne[65] est *identifiée* lorsque son identité ressort directement des données pertinentes[66].

Elle est *identifiable* lorsque les données permettent indirectement, par corrélation d'informations ou en raison du contexte, de déterminer à qui elles se rapportent[67]. Une possibilité d'identification purement théorique ne suffit pas[68]. Si l'identification nécessite des moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre, la personne concernée n'est pas identifiable

63 CR CP II-*Chappuis,* art. 321 CP N 71 ; *Corboz* (n. 55), art. 321 CP N 69.

64 En effet, tant les conditions générales d'UBS que de Credit Suisse précisent que si des données bancaires doivent être transmises à un prestataire sis à l'étranger, celles-ci « ne se réfèrent pas à l'identité du client », respectivement « ne permettent aucune déduction quant à l'identité du client » (conditions générales d'UBS de 2020, ch. 15 ; conditions générales de Credit Suisse 2019, ch. 15).

65 *De lege lata,* les données se rapportant tant à une personne physique qu'à une personne morale peuvent constituer des données personnelles (art. 3 let. b LPD). Le projet de révision totale de la LPD (ci-après « P-LPD ») propose de renoncer à la protection des données se rapportant aux personnes morales, ce qui mettrait fin à un particularisme suisse (art. 4 let. a P-LPD) ; pour une critique de l'exclusion des personnes morales de la future LPD, cf. *Hirsch Célian,* L'accès aux données d'une procédure au regard de la LPD, Jusletter du 17 septembre 2018, N 127 ss ; cf. également Message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6595 (ci-après « Message P-LPD »).

66 Message du Conseil fédéral concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988, FF 1988 421, 452 (ci-après « Message LPD ») ; ATF 138 II 346, c. 6.1 ; ATF 136 II 508, c. 3.2 ; Tribunal administratif fédéral A-7183/2008 du 7 mai 2009, c. 5.2.2 ; *Blechta Gabor-Paul,* in : Maurer-Lambrou Urs/Blechta Gabor-Paul (édit.), BSK – Datenschutzgesetz und Öffentlichkeitsgesetz, art. 3 LPD N 8 ss ; *Meier Philippe,* Protection des données – Fondements, principes généraux et droit privé, Berne 2010, N 431 s. ; *Rosenthal David/Jöhri Yvonne,* Handkommentar zum Datenschutzgesetz, Zurich 2008, art. 3 LPD N 20. Par exemple, une pièce d'identité permet l'identification directe de la personne concernée (ATF 138 II 346, c. 6.1). Selon *Probst,* une carte de visite identifie également directement la personne concernée (*Probst Thomas,* Die unbestimmte « Bestimmbarkeit » der von Daten betroffenen Personen im Datenschutzrecht, PJA 2013, p. 1423 ss (ci-après : *Probst,* Bestimmbarkeit [n. 66]), p. 1429 s.).

67 *Ibid*. Par exemple, il peut être possible d'identifier la personne figurant sur une photographie même si son visage est flouté, au regard du lieu et/ou du contexte de la prise de vue (ATF 138 II 346, c. 6.2 ss). Une adresse IP permet dans certaines circonstances l'identification de la personne concernée (ATF 136 II 508, c. 3.5), cf. également *Infra* section II.3 et n. 89. Du point de vue du droit européen CJUE, arrêt du 19 octobre 2016, C-582/14, Patrick Breyer c. Allemagne.

68 *Ibid*.

au sens de la LPD[69]. Dans ce contexte, on prend en compte notamment l'intérêt que présente l'identification[70], ainsi que les moyens techniques facilitant la détermination de la personne concernée (tels que les moteurs de recherche) à leur disposition[71].

Des procédés techniques[72] peuvent empêcher la réidentification de la personne concernée. La doctrine juridique distingue généralement l'anonymisation des données de leur pseudonymisation[73]. Dans les paragraphes qui suivent, nous examinons ces deux notions et les conséquences de tels procédés en droit.

2. Données anonymisées

L'anonymisation a pour but d'empêcher définitivement quiconque, y compris l'auteur du traitement, de rattacher les données à une personne déterminée[74]. Dans la mesure où, par définition, l'anonymisation rend impossible la réidentification de la personne concernée, les données anonymisées ne constituent pas des données personnelles et échappent au champ d'application de la LPD[75].

Cela étant, en pratique, il est fréquemment difficile de déterminer quelles mesures techniques suf-

69 Message LPD (n. 66), p. 452 ; ATF 138 II 346, c. 6.1 ; 136 II 508, c. 3.2 ; Tribunal administratif fédéral A7183/2008 du 7 mai 2009, c. 5.2.2 ; BSK DSG-*Blechta* (n. 66), art. 3 LPD N 11 ; *Rosenthal/Jöhri* (n. 66), art. 3 LPD N 24 ss ; *Rosenthal David,* Personendaten ohne Identifizierbarkeit?, digma 2017, p. 198 ss, p. 199 s. ; *Meier* (n. 66), N 433. A titre d'exemple, la personne concernée n'est généralement pas identifiable lorsque son identification requerrait l'analyse sophistiquée d'une statistique (Message LPD [n. 66], p. 452).

70 *Ibid*. Ainsi, une correspondance officielle évoquant généralement le processus de sélection des diplomates ne rend pas identifiable un candidat malheureux au concours diplomatique, lorsque l'identification présupposerait de recouper les informations contenues dans cette correspondance avec une liste de candidats gardée confidentielle. En effet, ces efforts apparaissent disproportionnés par rapport à l'intérêt que revêt l'identification pour un tiers (arrêt du Tribunal administratif fédéral A-7183/2008 du 7 mai 2009). Précisons qu'il n'est pas toujours facile de déterminer le point de vue duquel la possibilité d'identification doit être analysée (pour un résumé de la problématique et des points de vue adoptés en doctrine et dans la jurisprudence, cf. *Probst,* Bestimmbarkeit [n. 66], p. 1431 ss). A titre d'exemple, *Probst* mentionne le numéro d'assuré (souvent appelé « numéro AVS » dans le langage courant) : le numéro d'assuré constitue désormais une suite de chiffres aléatoires. La possibilité d'identifier la personne concernée dépend ainsi des autres informations disponibles, ce pourquoi l'analyse apparaît différente selon qu'on se positionne du point de vue de l'employeur de la personne concernée ou de celui d'un tiers (*Probst,* Bestimmbarkeit [n. 66], p. 1426). Nous examinerons plus en détail cette problématique dans le contexte particulier de la pseudonymisation, cf. *infra* section II.3.

71 *Ibid*. On pense ainsi en premier lieu à la possibilité d'opérer des recoupements avec d'autres sources d'information ; cf. *Probst Thomas,* Die Verknüpfung von Personendaten und deren Tragweite, in : Epiney Astrid/Probst Thomas/Gammenthaler Nina (édit.), Datenverknüpfung, Problematik und rechtlicher Rahmen, Zurich/Bâle/Genève 2011 (ci-après : *Probst,* Verknüpfung [n. 71]), p. 19 ; ainsi que *Probst,* Bestimmbarkeit (n. 66), p. 1425. Cela étant, les moyens pertinents peuvent également inclure le recours à un tiers, y compris une autorité (ATF 136 II 508, c. 3.5 et réf. citées). Ainsi, l'ouverture d'une procédure pénale contre inconnu constitue dans certaines circonstances un moyen raisonnable d'identifier le titulaire d'une adresse IP (ATF 136 II 508, c. 3.5).

72 Cf. Avis 05/2014 du Groupe de travail « Article 29 » sur la protection des données (remplacé par le Comité Européen de la Protection des Données [EDPB] à compter du 25 mai 2018) sur les techniques d'anonymisation du 10 avril 2014 (« Avis 05/2014 Groupe de travail Article 29 ») pour des exemples de procédés techniques envisageable et une analyse des risques juridiques inhérents à ceux-ci.

73 *Probst,* Verknüpfung (n. 71), p. 17 s. ; *Rosenthal/Jöhri* (n. 66), art. 3 N 34 ; précisons que ces notions sont issues de la doctrine juridique et recouvrent une variété de procédés informatiques. À titre d'exemple, *Meier* cite le cryptage à sens unique (*Meier* [n. 66], N 437). Le cryptage consiste à transformer les données en une forme qui ne peut être interprétée qu'au moyen d'un élément secret, la clé (cf. Glossaire publié par le Préposé <*https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/generalites/glossaire.html*>). Selon la position adoptée ici (approche relative, cf. *infra* section II.3), les données cryptées ne constituent en principe pas des données personnelles pour celui qui ne dispose pas de la clé.

74 *Baeriswyl Bruno,* Big Data zwischen Anonymisierung und Re-Individualisierung, ZIK 59/2014, p. 50 ss ; *Probst,* Verknüpfung (n. 71), p. 13 s. ; *Rosenthal/Jöhri* (n. 66), art. 3 LPD N 35 ; *Rudin Beat,* Commentaire Stämpfli LPD, art. 3 N 13 ; *Schweizer Rainer J./Bischof Severin,* Der Begriff der Personendaten, digma 2011, p. 152 ss, p. 155. *Probst* relève qu'aucune loi ne définit l'anonymisation, mais qu'un certain nombre de dispositions légales imposent d'anonymiser des données, ainsi l'art. 9 LTrans, l'art. 14*a* LSF, et l'art. 12 de la Loi sur le recensement.

75 *Baeriswyl* (n. 74), p. 53 ; *Rosenthal/Jöhri* (n. 66), art. 3 N 38 ; *Rudin* (n. 74), art. 3 N 13 ; *Schweizer/Bischof* (n. 74), p. 155.

fisent – quel *degré* d'anonymisation est nécessaire – pour éliminer effectivement toute possibilité de réidentification[76]. À ce propos, il sied de rappeler qu'une possibilité d'identification purement théorique ne suffit pas pour considérer que la personne concernée est identifiable au sens de la LPD. Ainsi, les données anonymisées ne constituent plus des données personnelles si, selon le cours ordinaire des choses, aucun intéressé ne mettait en œuvre les moyens raisonnablement susceptibles d'être utilisés pour la réidentification[77].

Afin de déterminer si les données sont suffisamment anonymisées pour éviter l'application de la LPD, la banque qui entend transmettre des données à un prestataire de services *cloud* devra ainsi prendre en considération les moyens de réidentification dont disposent le prestataire ou tout autre tiers autorisé[78] (par exemple les éventuelles informations complémentaires à leur disposition) et leur intérêt à la réidentification (par exemple au regard de la valeur des données transmises dans le pays de destination du point de vue politique ou fiscal).

3. Données pseudonymisées

Le terme « pseudonymisation » désigne les procédés par lesquels un identifiant neutre est substitué aux éléments permettant une identification directe[79]. Certains individus autorisés conservent la possibilité de réidentifier la personne concernée en réalisant l'opération inverse[80]. Ainsi, par définition, certaines personnes sont en mesure d'identifier à qui se rapportent les données pseudonymisées, tandis que d'autres en sont incapables[81]. En pratique, la pseudonymisation est notamment utilisée dans le cadre de transferts de données, notamment à l'étranger : l'auteur du traitement conserve alors le moyen d'identifier la personne concernée, tandis que le récipiendaire a accès uniquement aux pseudonymes.

La qualification juridique des données pseudonymisées est débattue en doctrine. Dans ce contexte, la question-clé est celle de savoir *de quel point de vue* il convient d'apprécier la possibilité de réidentifier la personne concernée[82]. Bien que la doctrine suisse soit généralement peu développée sur ce point, elle se réfère régulièrement à la controverse entre la théorie absolue et la théorie relative de l'identifiabilité élaborée par les auteurs européens[83] : selon l'approche dite *absolue* ou *alternative*, il suffit qu'une seule partie

76 De nombreux auteurs soulignent au demeurant qu'une anonymisation complète et irréversible apparaît difficilement réalisable au regard de l'évolution technologique et des quantités de données disponibles pour opérer des recoupements, cf. p. ex. *Baeriswyl* (n. 74), p. 51 et 54 ; *Rosenthal/Jöhri,* Handkommentar, art. 3 LPD N 38 ; *Rudin* (n. 74), art. 3 N 13 ; *Schweizer/Bischof* (n. 74), p. 156. A titre d'exemple, *Rosenthal/Jöhri* relèvent que la suppression par une banque de l'ensemble des données identifiant directement le client ne suffit pas nécessairement à anonymiser irréversiblement les données afférentes à son compte bancaire. En effet, la réidentification par le recoupement des transactions figurant sur l'extrait de compte avec les données publiées en matière de publicité des participations dans les sociétés cotées ne peut être exclue. De façon similaire, il peut être possible d'identifier la personne figurant sur une prise de vue publiée sur Google Street View même si son visage est flouté, au regard du lieu et/ou du contexte de la prise de vue (ATF 138 II 346, c. 6.2 ss, cf. également n. 67 *supra*).

77 Cf. consid. 26 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (RGPD) ; certains auteurs qualifient une telle situation d'« anonymisation de facto », cf. p. ex. *Meier* (n. 66), N 440 ss.

78 Nous analysons la question des (éventuels) récipiendaires à prendre en comptes plus en détail en lien avec les données pseudonymisées (section II.3). Les mêmes développements s'appliquent *mutatis mutandis* également aux données pseudonymisées.

79 Par exemple, le remplacement d'un nom par un alias ou un numéro. Cf. *Meier* (n. 66), N 446 ; *Probst,* Verknüpfung (n. 71), p. 17 ; *Rosenthal/Jöhri* (n. 66), art. 3 LPD N 36 s. ; *Schweizer/Bischof* (n. 74), p. 156. Concernant les diverses mesures techniques de pseudonymisation, le G29 mentionne également le système cryptographique à clé secrète, la fonction de hachage, la fonction de hachage par clé avec clé enregistrée, le chiffrement déterministe ou fonction de hachage par clé avec suppression de la clé ou encore la tokenization, laquelle est appliquée dans le secteur financier (G29, Avis 05/2014 sur les Techniques d'anonymisation, p. 22 s.).

80 Par exemple, en se référant à une table de concordance entre le pseudonyme et l'identifiant ou au moyen d'un algorithme de cryptage à double sens, cf. *Meier* (n. 66), N 446.

81 *Probst,* Verknüpfung (n. 71), p. 17 ; *Rudin* (n. 74), art. 3 N 14.

82 *Probst,* Bestimmbarkeit (n. 66), p. 1426.

83 *Meier* (n. 66), N 445 ; *Weber Rolf H./Fercsik Schnyder Orsolya,* « Was für 'ne Sorte von Geschöpf ist euer Krokodil ? » – Zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic ! 2009, p. 577 ss, p. 582.

(par exemple soit l'expéditeur des données, soit leur récipiendaire) puisse identifier la personne à laquelle se rapportent les données pour que ces dernières constituent des données personnelles *erga omnes*[84]. Selon cette approche, les données pseudonymisées constitueraient en tout état des données personnelles, certains individus autorisés étant par définition en mesure de réidentifier la personne concernée. Par opposition, d'autres auteurs retiennent que la possibilité d'identifier la personne concernée s'apprécie de façon différenciée, selon le point de vue de l'intéressé (approche dite *relative*)[85]. Des données pseudonymisées pourraient ainsi constituer des données personnelles du point de vue des personnes en mesure d'inverser l'opération de pseudonymisation (par exemple l'auteur de cette opération), et non de celui de tiers (par exemple le récipiendaire des données pseudonymisées)[86].

Le Tribunal fédéral s'est penché sur une problématique comparable dans l'ATF 136 II 508 (arrêt dit « Logistep »). Nous pouvons résumer l'état de fait pertinent comme suit : au moyen de logiciels *ad hoc,* la société Logistep AG enregistrait certaines informations en lien avec le téléchargement d'œuvres protégées par le droit d'auteur téléchargées sur des réseaux *peer-to-peer,* y compris l'adresse IP du périphérique utilisé pour le téléchargement. Logistep vendait ces informations aux titulaires de droits d'auteur. Les titulaires de droits d'auteurs se fondaient sur les données fournies par Logistep pour porter plainte pénale contre inconnu. L'accès au dossier pénal leur permettait ensuite d'identifier le contrevenant, puis d'agir contre celui-ci sur le plan civil.

Dans ce contexte, le Tribunal fédéral a analysé la conformité de l'activité de Logistep à la LPD. En particulier, il s'agissait de déterminer si Logistep traitait des données personnelles au sens de la LPD. Logistep faisait en particulier valoir qu'elle était incapable d'identifier à qui les données (en particulier les adresses IP) collectées se rapportaient, seuls les titulaires de droits d'auteur étant en mesure de procéder à l'identification, et ce dans le cadre d'une procédure pénale[87].

Le Tribunal fédéral n'a toutefois pas suivi l'argumentation de Logistep sur ce point. Il a retenu que la possibilité d'identification s'analysait en principe du point de vue particulier du détenteur de l'information[88]. Dans le cadre de la transmission d'informations, il suffisait toutefois que le récipiendaire puisse identifier la personne concernée pour que les données constituent des données personnelles soumises à la LPD *pour les deux parties* à la transmission[89]. Par-

[84] Les autorités européennes en matière de protection des données se prononcent en faveur de l'approche absolue, cf. Avis 05/2014 Groupe de travail « Article 29 », p. 10 : « *[i]l est crucial de comprendre que, dans le cas où un responsable du traitement des données n'efface pas les données originales (identifiables) au niveau des événements individuels et transmet une partie de cet ensemble de données (par exemple après avoir supprimé ou masqué les données identifiables), l'ensemble de données résultant constitue encore des données à caractère personnel. Ce n'est que si les données sont agrégées par le responsable de leur traitement à un niveau où les événements individuels ne sont plus identifiables que l'ensemble de données résultant peut être qualifié d'anonyme. Par exemple : si une organisation collecte des données sur des déplacements individuels, les habitudes de voyage au niveau des événements individuels pourraient encore être considérées comme des données à caractère personnel pour toute partie intéressée, tant que le responsable du traitement des données (ou un tiers) continue à avoir accès aux données brutes originales, même si les identifiants directs ont été supprimés de l'ensemble de données transmis à des tiers. Mais si le responsable du traitement des données efface les données brutes et ne transmet à des tiers que des statistiques agrégées à un niveau supérieur, par exemple ‹le lundi, sur le trajet X, le nombre de passagers est supérieur de 160% à celui du mardi›, ces données pourraient être qualifiées d'anonymes* », ainsi que l'exemple cité en p. 16 s. Nous n'avons pas connaissance d'auteurs suisses se déclarant expressément en faveur de l'approche absolue. Cela étant, le Préposé s'est prononcé en faveur de l'application de la théorie absolue en ce qui concerne les données pseudonymisées, cf. 22e rapport d'activités du Préposé (2014/2015) – Externalisation à l'étranger de données bancaires pseudonymisées (<*https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/anciens-rapports/22e-rapport-d-activites-2014-2015/externalisation-a-letranger-de-donnees-bancaires-pseudonymisees.html*>).

[85] En ce sens *Probst,* Bestimmbarkeit (n. 66), p. 1429 s. ; *Rudin* (n. 74), art. 3 N 12.

[86] *Ibid*.

[87] ATF 136 II 508, c. 2.2. La possibilité d'identification était ainsi différente pour chacune des parties au transfert. En ce sens, l'état de faits de l'arrêt Logistep présente des similitudes avec le transfert de données pseudonymisées.

[88] ATF 136 II 508, c. 3.4 et réf. citées.

[89] *Ibid*. Le Tribunal fédéral a validé la possibilité d'identification *in casu,* les démarches nécessaires n'apparaissant pas disproportionnées au regard des intérêts en jeu (ATF 136 II 508, c. 3.5). Il souligne au demeurant que le modèle commercial de Logistep reposait précisément sur la possibilité d'identification *(ibid.)*. Cf. à cet égard également *supra* n. 67. Pour une discussion des autres questions de protection des données abordées dans l'arrêt Logistep, cf.

tant, les données traitées par Logistep constituaient des données personnelles.

La plupart des auteurs soutiennent que l'issue de l'arrêt Logistep est propre aux faits de la cause, ce pourquoi la portée de cet arrêt doit être relativisée[90]. Ce nonobstant, dans une prise de position[91] que la pratique semble avoir largement ignorée[92], le Préposé fédéral à la protection des données et à la transparence (ci-après le « Préposé ») l'a interprété comme entérinant l'analyse des possibilités d'identification selon l'approche alternative[93]. Selon cette prise de position du Préposé, il conviendrait dès lors de considérer en toutes circonstances les données pseudonymisées comme des données personnelles.

Dans un récent arrêt, le *Handelsgericht* retient que, pour autant que les mesures de pseudonymisation empêchent effectivement l'identification de la personne concernée, les données pseudonymisées ne constituent pas des données personnelles *pour celui qui n'a pas accès à la clé d'identification*[94]. Sur recours, le Tribunal fédéral fait sien ce raisonnement, sans commentaire[95].

Nous saluons la clarification théorique selon laquelle les données pseudonymisées ne constituent en principe[96] pas des données personnelles pour le destinataire qui n'a pas accès à la clé d'identification. Cette position nous paraît en adéquation avec la *ratio legis* de la LPD : en effet, la transmission de données qui ne permettent pas l'identification par le destinataire ne porte pas atteinte aux droits de la personnalité de la personne concernée[97]. De façon bienvenue, ces jurisprudences mettent ainsi fin à l'incertitude découlant de l'arrêt Logistep et de la prise de position du Préposé évoquée plus haut[98].

Une question importante pour la pratique est celle de savoir si la possibilité de réidentification s'apprécie du seul point de vue du destinataire des données, ou s'il convient de considérer également celui des tiers qui pourraient obtenir l'accès aux données. En particulier, la banque qui transmet des données pseudonymisées à un prestataire de services à l'étranger doit-elle analyser la possibilité de réidentification par les autorités dans le pays de destination ? À notre connaissance, la doctrine ne s'est jamais penchée sur cette problématique précise. Selon nous, la réponse découle de l'interprétation téléologique de la LPD : cette loi a pour but de protéger les droits de la person-

p. ex. *Glarner Andreas/Rüfenacht Karin,* (Pyrrhus-)sieg für den Datenschutz, Jusletter du 20 décembre 2010 ; et *Rosenthal David,* Wenn Datenschutz übertrieben wird oder : Bad cases make bad law, Jusletter du 27 septembre 2010, N 6 ss ; *Rosenthal David,* Logistep : Offenbar ein Einzelfall, digma 2011, p. 40 ss, ci-après : *Rosenthal,* Logistep [n. 89]). S'agissant de l'exploitabilité en procédure pénale de preuves obtenues par des procédés semblables à ceux de la société Logistep, cf. arrêt de l'*Obergericht* bernois du 22 mars 2011, BK 11/9, CAN 2012/36, p. 102 ss. L'*Obergericht* du canton zurichois a laissé la question ouverte dans un arrêt du 3 février 2014, ZR 2014, p. 34 ss. S'agissant des implications de l'arrêt Logistep pour la responsabilité des fournisseurs d'hébergements, cf. *Francey Julien,* La responsabilité délictuelle des fournisseurs d'hébergement et d'accès Internet, Zurich 2017, N 647 ss.

90 En ce sens notamment : *Probst,* Bestimmbarkeit (n. 66), p. 1429 s. ; *Rosenthal,* Logistep (n. 89), p. 40 s.

91 22e rapport d'activités du Préposé (2014/2015) – Externalisation à l'étranger de données bancaires pseudonymisées (<*https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/anciens-rapports/22e-rapport-d-activites-2014-2015/externalisation-a-letranger-de-donnees-bancaires-pseudonymisees.html*>).

92 De nombreuses banques suisses ont notamment transmis de vastes volumes de données pseudonymisées aux autorités américaines dans le cadre du programme américain, cf. p. ex. 4A_365/2017 (n. 2).

93 22e rapport d'activités du Préposé (2014/2015) – Externalisation à l'étranger de données bancaires pseudonymisées (<*https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/anciens-rapports/22e-rapport-d-activites-2014-2015/externalisation-a-letranger-de-donnees-bancaires-pseudonymisees.html*>).

94 HG150170 (n. 2), c. 5.3.5.2 et c. 6.

95 TF 4A_365/2017 (n. 2), c. 5.2.2. Les praticiens semblent se satisfaire de cette approche. Par exemple, dans un litige ultérieur s'inscrivant également dans le cadre du Programme américain, le demandeur n'a pas contesté l'admissibilité de la transmission de données pseudonymisées, mais uniquement le caractère suffisant des mesures de pseudonymisation prises par la banque défenderesse (arrêt du Tribunal fédéral 4A_50/2019 du 28 mai 2019, c. 6.5).

96 Dans l'arrêt 4A_365/2017 (n. 2), le Tribunal fédéral n'opère pas expressément un revirement de jurisprudence par rapport à son arrêt Logistep. Il ne nous semble dès lors pas exclu que dans des circonstances particulières – comme celles ayant donné lieu à l'arrêt Logistep – le Tribunal fédéral analyse la possibilité de réidentification selon la théorie alternative.

97 La doctrine majoritaire se prononce également en ce sens, cf. *supra* section II.1.

98 22e rapport d'activités du Préposé (2014/2015) – Externalisation à l'étranger de données bancaires pseudonymisées (<*https://www.edoeb.admin.ch/edoeb/fr/home/documentation/rapports-d-activites/anciens-rapports/22e-rapport-d-activites-2014-2015/externalisation-a-letranger-de-donnees-bancaires-pseudonymisees.html*>).

nalité de la personne concernée[99] (art. 1 LPD). La pseudonymisation permet d'échapper au champ d'application de la LPD si les mesures prises empêchent l'identification de la personne concernée, de telle sorte que sa personnalité n'est plus touchée. Or, ceci présuppose à notre sens que les mesures de pseudonymisation prises empêchent l'identification non seulement par le destinataire, mais aussi par les autres tiers autorisés[100] à accéder aux données dans le pays de destination (en particulier les autorités)[101], pour autant que le risque d'accès et de réidentification par ceux-ci n'apparaisse pas purement théorique[102]. Il appartient dès lors à la banque d'analyser s'il existe une possibilité pratique de réidentification par les autorités du pays de destination au regard du droit local, des moyens technologiques à la disposition de celles-ci et de leur intérêt à la réidentification[103].

III. Fardeau de la preuve

1. Les faits générateurs de droits et les faits dirimants

L'art. 8 CC prévoit que chaque partie doit, si la loi ne prescrit le contraire, prouver les faits qu'elle allègue pour en déduire son droit. Afin de déterminer le fardeau de la preuve, on distingue traditionnellement les faits générateurs de droit *(rechtserzeugende Tatsachen),* les faits libératoires/destructeurs *(rechtsvernichtende, rechtsaufhebende Tatsachen)* et les faits dirimants *(rechtshindernde Tatsachen)*[104]. Alors que les premiers doivent être établis par celui qui entend exercer le droit qu'ils fondent[105], les faits libératoires sont à la charge du débiteur qui entend se libérer d'une obligation[106]. Enfin, les faits dirimants sont à la charge de la partie qui prétend l'extinction du droit litigieux ou sa paralysie[107]. La doctrine reconnait que la distinction entre faits générateurs de droit et faits dirimants est délicate[108].

2. La pseudonymisation et l'anonymisation comme faits dirimants ?

Pour prendre un exemple concret, il appartient au client de prouver que la banque a révélé des données protégées par le secret bancaire (faits générateurs de droit), mais cette dernière peut alors prouver qu'il existait un motif justificatif à cette révélation (faits

99 En particulier, les règles sur la communication de données à l'étranger visent à protéger la personne concernée contre des risque qui n'existeraient pas en cas de traitement en Suisse (Message LPD [n. 66], p. 458 s.). De tels risques existent également en cas de communication de données pseudonymisées, si le droit du pays de destination permet aux autorités locales d'accéder aux données et si ces autorités peuvent (vraisemblablement) réidentifier la personne concernée. La position soutenue ici nous paraît ainsi également cohérente d'un point de vue historique et systématique.

100 Par opposition, il ne nous semble pas approprié d'apprécier la possibilité de réidentification du point de vue de tiers non autorisés. D'une part, les risques découlant d'un éventuel accès non autorisé existent également en l'absence de communication des données. D'autre part, la prise en compte des possibilités de réidentification par des tiers indéterminés nous paraît contraire à la sécurité du droit. Ceci est sans préjudice de l'obligation pour la banque d'analyser les risques d'accès non autorisé sous l'angle de sa gestion des risques opérationnels, notamment en lien avec une exportation de données (cf. FINMA, Circulaire 2008/21, Cm 135.6 ss et Annexe 3 Cm 20).

101 L'analyse de *Probst* selon laquelle le détenteur des données doit prendre en compte la possibilité d'identification par le destinataire lorsqu'il doit raisonnablement s'attendre à une telle (ré)identification nous semble aller dans le même sens, cf. *Probst,* Bestimmbarkeit (n. 66), p. 1433 s.

102 Nous rappelons qu'une possibilité d'identification purement théorique n'est pas suffisante pour admettre le caractère identifiable de la personne concernée (Message LPD [n. 66], p. 452).

103 Cf. *supra* section I.1 et réf. citées. S'agissant des moyens techniques, il siéra à notre sens de prendre en compte en particulier les données à la disposition des autorités concernées pour opérer des recoupements. L'intérêt à l'identification dépendra notamment de l'existence de contribuables ou d'autres personnes revêtant un intérêt pour le pays de destination (p.ex. dissidents politiques) parmi les clients de la banque et de la politique fiscale du pays concerné.

104 BK ZGB-*Walter,* art. 8 CC N 254 ss ; BSK ZGB I-*Lardelli/Vetter,* art. 8 CC N 38 ; CR CC I-*Piotet,* art. 8 CC N 31 ; *Jungo Alexandra,* Zürcher Kommentar, Art. 8 ZGB – Beweislast, Zivilgesetzbuch, 3e éd., Genève/Zurich/Bâle 2018, N 192.

105 ATF 139 III 7, c. 2.2 ; BK ZGB-*Walter,* art. 8 CC N 265 ; *Steinauer Paul-Henri,* Le titre préliminaire du Code civil et Droit des personnes, 2e éd., Bâle 2009, N 703.

106 BK ZGB-*Walter,* art. 8 CC N 279 ; BSK ZGB I-*Lardelli/Vetter,* art. 8 CC N 56 ; *Steinauer* (n. 105), N 705.

107 ATF 139 III 7, c. 2.2 ; 5A_365/2017 (n. 2), c. 5.2.1 ; BK ZGB-*Walter,* art. 8 CC N 288 ; BSK ZGB I-*Lardelli/Vetter,* art. 8 CC N 56 ; CR CC I-*Piotet,* art. 8 N 31 ; *Steinauer* (n. 105), N 707.

108 BK ZGB-*Walter,* art. 8 CC N 291 ; BSK ZGB I-*Lardelli/Vetter,* art. 8 CC N 57 ; *Steinauer* (n. 105), N 708.

dirimants)[109]. La question devient néanmoins plus délicate lorsque la banque affirme que les données ne concernent pas le client en raison de leur pseudonymisation ou anonymisation. Appartient-il alors au client de démontrer que les données révélées le rendent identifiable (puisque cela constitue une condition à la naissance de son droit)[110] ? Ou appartient-il à la banque de prouver qu'elle a paralysé les droits du client en pseudonymisant ou anonymisant ses données, de telle sorte que celles-ci ne constitueraient plus des données personnelles ?

À notre connaissance, la doctrine relative à la protection des données ne s'est, à ce jour, pas penchée sur cette question.

2.1 La solution proposée par la jurisprudence

Selon l'arrêt susvisé du *Handelsgericht* zurichois, la banque défenderesse invoque un fait dirimant lorsqu'elle allègue que les données litigieuses ne constituent pas des données personnelles, en raison des mesures de pseudonymisation prises[111]. Partant, il incombe à la banque de démontrer que la pseudonymisation empêche effectivement la réidentification par le destinataire des données[112].

Sur appel, le Tribunal fédéral confirme cette répartition du fardeau de la preuve[113]. Il souligne que les données litigieuses dérivent indubitablement de données personnelles[114]. Lors du processus de pseudonymisation, la banque traite ainsi des données personnelles[115]. Elle entend remettre le résultat de ce traitement à un tiers, le Département de Justice américain (DoJ). En faisant valoir que la transmission des données litigieuses échapperait au champ d'application de la LPD parce que les mesures de pseudonymisation prises empêcheraient l'identification des personnes concernées par le DoJ, la banque invoque bien une exception[116]. Elle supporte dès lors le fardeau de la preuve correspondante[117].

À notre avis, c'est à bon droit que le *Handelsgericht* et le Tribunal fédéral font supporter au demandeur le fardeau de la preuve de l'existence de données personnelles en main du défendeur *(faits générateurs de droit),* mais n'exigent pas qu'il prouve que ces données constituent encore des données person-

109 *Steinauer* prend précisément l'exemple d'une atteinte à la personnalité qui doit être établie par le lésé (art. 28 al. 1 CC), mais dont l'auteur peut opposer un motif justificatif (art. 28 al. 2 CC) (*Steinauer* [n. 105], N 707). En matière de transmission de données, cf. arrêts du Tribunal fédéral 4A_588/2018 du 27 juin 2019 et 4A_50/2019 du 28 mai 2019. Nous relevons que celui à qui incombe la preuve supporte également le fardeau de l'allégation. En particulier, il appartient au prétendu lésé d'alléguer précisément quelles données personnelles auraient été transmises à l'étranger, et dans quel contexte (TF 4A_588/2018, c. 4.3.2). Selon le Tribunal fédéral, le demandeur ne peut se contenter d'alléguer que la banque défenderesse aurait transmis ses données personnelles et de produire 300 pages de documentation transmises au DoJ, sans autre précision quant au contexte de la transmission de données (étant précisé qu'en l'espèce, la banque avait livré des données au DOJ à plusieurs reprises) et quant aux parties de la documentation censées contenir des données personnelles (TF 4A_588/2018, c. 4.3.3 s.). Au stade des mesures provisionnelles visant à interdire une transmission de données, il suffit que le lésé rende l'atteinte à sa personnalité vraisemblable (TF 4A_50/2019, c. 6.6). Par opposition, le Tribunal fédéral semble pencher pour exiger la preuve stricte du motif justificatif *(Ibid.)*. La question a toutefois été laissée ouverte *(Ibid.)*.

110 Telle était la position adoptée par la banque dans son recours auprès du Tribunal fédéral dans l'affaire zurichoise susmentionnée (n. 2), cf. TF 4A_365/2017 (n. 2), c. 5.2.

111 HG150170 (n. 2), c. 5.3.5.8.

112 *Ibid*.

113 TF 4A_365/2017 (n. 2), c. 5.2.1 ss.

114 TF 4A_365/2017 (n. 2), c. 5.2.2.

115 *Ibid*.

116 *Ibid*.

117 *Ibid*. S'agissant plus précisément de l'objet de la preuve, le *Handelsgericht* considère pour l'essentiel que la banque aurait dû démontrer les aspects suivants (HG150170 [n. 2], c. 5.3.5.5 ss) : (1) les mesures prises pour limiter l'accès à la clé de concordance ; (2) l'impossibilité pour les autorités américaines de réidentifier la personne concernée au moyen des données transmises ; et (3) l'impossibilité pour les autorités américaines de réidentifier la personne concernée en opérant des recoupements entre les données transmises et d'autres informations à leur disposition. Précisons que, s'agissant du premier point, le Tribunal fédéral se montre moins exigeant et considère que l'utilisation d'un numéro de compte pseudonymisé constitue en principe une mesure propre à empêcher la réidentification. En effet, suite à cette mesure, la réidentification présuppose le recours à la clé de concordance, à laquelle le DoJ n'a pas accès (TF 4A_365/2017 [n. 2], c. 5.3.1). Par ailleurs, le Tribunal fédéral laisse expressément ouverte la question de savoir qui, de la banque ou du demandeur, supporte le fardeau de la preuve s'agissant du troisième point (possibilité d'opérer des recoupements extrinsèques) (TF 4A_365/2017 [n. 2], c. 5.2.2 *in fine*). Dans le même sens que le *Handelsgericht,* cf. un arrêt récent de l'*Appellationsgericht* du canton de Bâle-Ville (ZB.2019.3 du 6 septembre 2019, c. 4.2.3) sur lequel nous revenons ci dessous (*infra* n. 127).

nelles au jour de sa demande. En effet, le défendeur invoque alors une paralysie du droit du demandeur en affirmant qu'il les a pseudonymisées ou anonymisées *(faits dirimants)*.

La preuve de ces faits dirimants est néanmoins difficile à apporter en pratique. En effet, nous l'avons vu[118], les données ne sont pseudonymisées ou anonymisées que si un tiers ne peut pas réidentifier les personnes concernées en fonction des moyens raisonnablement susceptibles d'être utilisés et de son intérêt à la réidentification. Il appartient alors au défendeur de prouver que le destinataire des données pseudonymisées ou anonymisées, voire un tiers qui pourrait également avoir accès à ces données par la suite, ne disposerait pas de ces moyens ou n'aurait pas d'intérêt à la réidentification. Le défendeur devrait ainsi apporter la preuve stricte d'un fait négatif, ce qui est généralement impossible[119].

Selon certains auteurs, il se justifie de renverser le fardeau de la preuve en présence d'un fait négatif[120]. Cela étant, le Tribunal fédéral maintient en général le fardeau de la preuve et recourt à deux constructions juridiques distinctes qui relativisent l'impossibilité pratique de prouver un fait négatif :

– le demandeur peut se voir imposer un devoir de collaboration selon les règles de la bonne foi[121] afin de prouver un fait positif qui empêche la réalisation du fait négatif pertinent[122]. À défaut, le tribunal doit en principe considérer que le fait négatif est prouvé[123];
– la charge de la preuve peut être allégée en raison d'un « état de nécessité en matière de preuve » *(Beweisnot)*[124] ; le degré de preuve requise se limite alors à la vraisemblance prépondérante[125].

2.2 Une solution plus nuancée

À notre avis, il convient d'exiger un degré de preuve distinct pour chacun des faits dirimants que doit établir la banque en cas de communication de données anonymisées ou pseudonymisées[126] :

– les mesures prises pour limiter *l'accès à la clé d'identification* constituent un fait positif et doivent dès lors faire l'objet d'une preuve stricte ;
– l'impossibilité pour le destinataire et/ou les tiers pertinents de réidentifier la personne concernée au moyen des données transmises *(recoupements intrinsèques)* est un fait négatif, mais le périmètre de la preuve reste clairement déterminé. Partant, cet élément peut être établi avec un haut degré de vraisemblance, notamment au moyen de tests techniques, et aucun allégement particulier du fardeau de la preuve n'est nécessaire ;
– l'impossibilité pour le destinataire et/ou les tiers pertinents de réidentifier la personne concernée en opérant des recoupements entre les données transmises et d'autres informations à leur disposition *(recoupements extrinsèques)* constitue un fait négatif indéterminé. La preuve correspondante présuppose que la banque puisse établir une liste exhaustive des informations extrinsèques dont disposent le destinataire et/ou les tiers pertinents, et délimiter précisément quelles déductions peuvent être tirées des recoupements entre ces informations et les données transmises. Or, il n'est pas réaliste d'exiger de la banque la démonstration d'éléments d'une telle envergure. Dans ces circonstances, il convient d'exiger de la partie adverse la preuve que le destinataire et/ou les tiers pertinents disposent de certaines informations supplémentaires et peuvent – à tout le moins sous l'angle de la vraisem-

118 Cf. *supra* sections III.2 et III.3.
119 CR CC I-*Piotet,* art. 8 N 53.
120 *Steinauer* (n. 105), N 714 et réf. citées.
121 CR CC I-*Piotet,* art. 8 N 53 ; BK ZGB-*Walter,* art. 8 CC N 353 ; *Steinauer* (n. 105), N 715.
122 ATF 119 II 305 ; 106 II 31 ; 98 II 231 ; *Steinauer* (n. 105), N 715. S'agissant de notre problématique, le défendeur devrait ainsi apporter la preuve que le destinataire ou un éventuel tiers auraient des moyens ainsi qu'un intérêt à réidentifier les données le concernant.
123 *Steinauer* (n. 105), N 715. Le Tribunal fédéral, plus nuancé, retient que le juge peut considérer le défaut de preuve du fait positif comme un « indice » que le fait négatif est prouvé (ATF 98 II 231, c. 5).
124 ATF 138 III 81, c. 4.2.2 ; plus récemment, cf arrêt du Tribunal fédéral 4A_594/2017 du 13 novembre 2018, c. 5.1.
125 A noter que la vraisemblance prépondérante *(die überwiegende Wahrscheinlichkeit)* se distingue de la simple vraisemblance *(die Glaubhaftmachung)* (ATF 138 III 81, c. 4.2.2).
126 S'agissant de l'objet de la preuve, cf. HG150170 (n. 2), c. 5.3.5.5 ss et TF 4A_365/2017 (n. 2), c. 5.3.1 et *supra* n. 117.

blance prépondérante – en déduire l'identité de la personne concernée[127].

IV. Quelques suggestions pour la pratique bancaire

Selon nous et sans prétendre à l'exhaustivité, les banques qui entendent transmettre des données bancaires anonymisées ou pseudonymisées à l'étranger, que cela soit de l'*outsourcing* ou dans le cadre du *cloud banking,* seraient bien avisées de prendre les précautions suivantes, au regard des développements qui précèdent :

- limiter l'accès à la clé d'identification aux personnes qui en ont besoin (principe *need-to-know*), documenter les restrictions mises en place et protéger la clé contre les accès non autorisés ;
- confirmer au moyen de tests techniques l'impossibilité de déduire l'identité du client des données transférées (recoupements intrinsèques) et documenter la méthode utilisée ainsi que le résultat des tests ;
- se renseigner quant aux droits d'accès aux données dont pourraient bénéficier des tiers (en particulier les autorités locales) dans la juridiction de destination ;
- analyser le risque que le destinataire et/ou tout tiers autorisé (en particulier les autorités locales) puisse réidentifier le client au moyen de recoupement entre les données transférées et d'autres données à leur disposition (recoupements extrinsèques). Dans ce contexte, il conviendra à notre sens de prendre en compte notamment la nature et l'étendue des autres informations dont dispose vraisemblablement le destinataire des données et/ou le tiers pertinent, ainsi que l'intérêt que revêt la réidentification pour ce dernier. L'intérêt à la réidentification des autorités qui pourraient accéder aux données selon le droit local dépendra en particulier de la présence de contribuables du pays concerné au sein de la clientèle de la banque et de la politique fiscale dudit pays ;
- selon le risque de réidentification, obtenir le consentement préalable du client et sa renonciation au secret bancaire par la révision des conditions générales de la banque. Dans ce cadre, la nécessité de fournir au client des informations suffisantes pour un consentement valable est susceptible d'entrer en tension avec les besoins opérationnels de la banque. En effet, d'un point de vue tant pratique que commercial, la révision des conditions générales constitue un exercice délicat. La banque souhaitera dès lors vraisemblablement conserver une certaine flexibilité quant aux destinataires des données et aux juridictions de destination, afin d'éviter de devoir modifier ses conditions générales lors de chaque externalisation[128].

[127] Du point de vue dogmatique, on peut fonder cette exigence sur un renversement du fardeau de la preuve (étant précisé que le Tribunal fédéral a expressément laissé ouverte la question de la répartition du fardeau de la preuve sur ce point, TF 4A_365/2017 [n. 2], c. 5.2.2 *in fine)*, sur le devoir de collaboration de la partie adverse, ou sur l'allégement du fardeau de la preuve en situation de *Beweisnot*. En pratique, ces trois théories nous semblent aboutir substantiellement au même résultat. Comme précédemment évoqué (cf. n. 117), un arrêt récent de l'*Appellationsgericht* du canton de Bâle-Ville (ZB.2019.3 du 6 septembre 2019, c. 4.2.3) retient au contraire que la banque supporte le fardeau de la preuve quant à l'impossibilité pour le DoJ d'effectuer des recoupements extrinsèques. Selon l'*Appellationsgericht,* cette décision s'impose parce que l'efficacité des mesures de pseudonymisation dépend des informations supplémentaires que possède le DoJ. L'*Appellationsgericht* rappelle néanmoins qu'une partie peut se voir imposer un devoir de collaboration selon les règles de la bonne foi afin de prouver un fait positif qui empêche la réalisation du fait négatif pertinent (ZB.2019.3 du 6 septembre 2019, c. 4.3.4). En l'espèce, la banque n'a pas allégué avant le dépôt de sa duplique le fait que les données litigieuses étaient pseudonymisées ; il ne pouvait être ainsi imposé à sa partie adverse, selon les règles de la bonne foi, d'apporter les éléments de preuve nécessaires pour prouver l'allégation inverse, à savoir la possibilité pour le DoJ de procéder à des recoupements extrinsèques (ZB.2019.3 du 6 septembre 2019, c. 4.3.4).

[128] En pratique, les banques recourent fréquemment à des formulations relativement ouvertes dans leurs conditions générales, par exemple en faisant référence à toutes les juridictions où se situent des filiales du groupe bancaire pertinent ou en énumérant diverses catégories de mandataires susceptibles de se voir communiquer des données client. Si l'analyse de telles pratiques dépasse le cadre de la présente contribution, l'arrêt du *Handelsgericht* (n. 2) illustre les risques inhérents à un consentement contractuel jugé insuffisant.

V. Conclusion

Les données bancaires sont en principe protégées tant par la LPD que par le secret bancaire. Les développements juridiques récents en la matière révèlent deux tendances opposées : d'une part la relativisation du secret bancaire, et d'autre part le renforcement des exigences en matière de protection des données. Cela étant, la LPD et le secret bancaire reposent sur un même fondement, la protection de la personnalité. De nombreux concepts communs sous-tendent ces deux domaines du droit. L'unicité de l'ordre juridique et l'interprétation systématique conduiront en général à interpréter un même concept de façon similaire en matière de protection des données et de secret bancaire. Les développements en matière de protection des données tendent de ce fait à influencer les exigences applicables en vertu du secret bancaire et vice-versa.

Ainsi, selon notre analyse, tant la LPD que le secret bancaire s'appliquent uniquement si les données bancaires permettent l'identification de la personne concernée. Pour échapper à cette double protection, la banque peut donc recourir à la pseudonymisation ou l'anonymisation des données. Ces méthodes ne sont néanmoins efficaces que lorsque ni le destinataire ni les éventuels tiers autorisés ne peuvent réidentifier les personnes concernées à l'aide de moyens raisonnablement susceptibles d'être utilisés, au regard de leur intérêt à la réidentification.

Il incombe à tout le moins partiellement à la banque de prouver qu'une telle réidentification est *(de facto)* impossible. À notre sens, il convient d'exiger de la banque la preuve stricte des mesures prises pour limiter l'accès à une éventuelle clé d'identification et de l'impossibilité d'identifier la personne concernée en recoupant entre elles les données communiquées. Par opposition, il appartiendra selon nous au demandeur de rendre vraisemblable que le tiers pourrait l'identifier au moyen de recoupements entre les données communiquées et d'autres informations à sa disposition.

Comme l'illustre la récente jurisprudence, l'apport des preuves pertinentes par la banque peut s'avérer difficile en pratique. À notre sens, la prudence impose une analyse des risques liés au traitement et la prise de diverses précautions préalablement au transfert de données.

Lorsque les données permettent son identification, le client peut consentir au traitement, respectivement renoncer au secret bancaire. Avec une partie de la doctrine existante, nous retenons que la validité du consentement présuppose la remise des mêmes informations au client au regard de la LPD qu'au regard du secret bancaire. Il s'agira en particulier d'informer le client de la finalité de la transmission de données, des catégories de destinataires, et des juridictions de destination.

Dans les paragraphes qui précèdent, nous avons formulé certaines suggestions correspondantes pour la pratique bancaire.

On peut se demander si à l'avenir le droit de la protection des données et le secret bancaire continueront à évoluer de concert. Au moment où nous écrivons ces lignes, le Parlement examine le projet de révision complète de la LPD. Ce projet prévoit que seules les données de personnes physiques seront protégées comme données personnelles[129]. Par opposition, tant les personnes morales que les personnes physiques pourront continuer à se prévaloir du secret bancaire. Ceci contribuera-t-il à une revalorisation du secret bancaire ? Par ailleurs, le P-LPD renforce les exigences en matière de devoir d'information et de consentement[130]. Cette évolution aura-t-elle des répercussions pour la renonciation au secret bancaire, ou sera-t-il désormais plus facile d'être délié du secret bancaire que d'obtenir le consentement au traitement de données personnelles ? Si nous ne prétendons pas déterminer les réponses à ces questions dans un cadre juridique en évolution, nous recommandons vivement au praticien bancaire de rester à l'affût des développements législatifs en matière de protection des données et de s'interroger sur leurs éventuelles conséquences pour le secret bancaire.

[129] Art. 2 al. 1 P-LPD. Précisons qu'en l'état des délibérations parlementaires, ce point ne semble plus faire débat.

[130] Art. 5 al. 6 et art. 14 al. 1 let. a P-LPD.