walderwyss avocats

Walder Wyss SA
Seefeldstrasse 123
Case Postale
8034 Zurich
Suisse

Téléphone +41 58 658 58 58
Fax +41 58 658 59 59
www.walderwyss.com

Rapport d'experts

Préparé pour	Association suisse des banquiers (ASB)
de	Walder Wyss SA (Dr. Michael Isler, Oliver M. Kunz. Dr. Thomas Müller, Dr. Jürg Schneider, Dr. David Vasella)
Concerne	**Admissibilité sous l'angle de l'art. 47 LB de la communication de données bancaires par des banques suisses à des mandataires étrangers**
	[Traduction du texte original allemand]
Date	15 février 2019 / 9101398v1

Table des matières

1. Contexte

1 L'Association suisse des banquiers (ASB) nous a demandé de préparer le présent rapport afin de répondre à la question suivante :

> *Une banque suisse viole-t-elle le secret bancaire au sens de l'art. 47 al. 1 et 2 de la Loi fédérale sur les banques et les caisses d'épargne (**LB**) lorsqu'elle transmet des données bancaires à un destinataire situé à l'étranger dans le cadre de l'exécution d'un mandat ?*

2 Les développements effectués dans le présent rapport se limitent à répondre à cette question. Les points suivants ne sont pas abordés :

(a) le champ d'application matériel de l'art. 47 LB ;

(b) la loi fédérale sur la protection des données (**LPD**) ;

(c) les dispositions en matière de secret autres que l'art. 47 al. 1 et 2 LB, telles que l'art. 273 du Code pénal suisse (**CP**) ou l'art. 35 LPD ; et

(d) le droit étranger.

3 La question à traiter doit être comprise dans le contexte du projet préliminaire de l'ASB intitulé « *Guide "Cloud" – Recommandations pour sécuriser le cloud banking* » (le **Guide**). Dans le présent rapport, les références à ce Guide sont faites à titre d'exemple. Nous ne nous prononçons pas sur l'exhaustivité et la pertinence des mesures techniques et organisationnelles contenues dans le Guide, ni sur la question de savoir quelle combinaison de mesures est appropriée dans un cas spécifique. Le Guide ne prétend, d'ailleurs, aucunement à une quelconque exhaustivité et précise que les banques, au moment d'appliquer le Guide, doivent prendre en compte leur taille ainsi que la complexité de leur modèle d'affaires, selon une approche basée sur les risques et proportionnée.

4 Dans ce rapport, nous parlons d' « externalisation » ou d' « intervention d'une personne auxiliaire » et entendons par là qu'une banque utilise les services d'un prestataire informatique - par exemple un fournisseur de *cloud computing* - et que ce dernier a ou peut avoir accès à des informations soumises au secret bancaire. Les questions techniques telles que les différents modèles de services ne sont traitées que de manière très superficielle.

2. Conclusions

5 Nous sommes d'avis que le recours à un auxiliaire par une banque et la révélation de **CID** (i.e. « données d'identification du client ») à ce dernier est admissible, à condition que :

(a) ce recours à un auxiliaire réponde à un intérêt raisonnable de la banque qui externalise, que l'auxiliaire assiste la banque dans son activité commerciale en étant soumis aux instructions de cette dernière, et que la banque – dans l'ensemble – continue à fournir elle-même de manière prépondérante les services convenus avec le client ; et

(b) il ne résulte d'aucun accord exprès ou tacite avec le client que le recours à un auxiliaire est interdit.

6 Ceci découle avant tout de l'art. 68 du Code des obligations suisse (**CO**). Dans la mesure où rien ne permet de limiter l'application de ce du principe prévu à cette disposition aux problématiques suisses, celui-ci s'applique dès lors également lorsqu'une banque externalise le traitement de CID auprès d'un prestataire de services à l'étranger, respectivement lorsque le prestataire de service étranger se voit octroyer un accès aux CID dans le cadre de son activité pour la banque. Sur cette base, nous estimons dès lors que, sous l'angle du droit privé, une banque peut également externaliser le traitement de CID auprès d'un prestataire de services étranger, par exemple dans le cadre d'une solution « cloud », et ce même si le prestataire a ou peut prendre connaissance de CID dans ce contexte.

7 Le secret bancaire (art. 47 al. 1 et 2 de la Loi sur les banques, **LB**) doit être compris comme un renforcement pénal des obligations de confidentialité prévues par le droit privé. Partant, si une banque a procédé à une externalisation autorisée sous l'angle contractuel, cette dernière est également autorisée à procéder à une telle externalisation sur le plan pénal, raison pour laquelle les conclusions exposées ci-dessus trouvent également application en matière pénale. Le recours à un prestataire de services et la révélation de CID à ce dernier sont donc généralement admissibles en vertu de l'art. 47 LB, et ce même si le prestataire de services est situé à l'étranger. Si, en revanche, un accord contractuel entre la banque et le client interdit l'externalisation du traitement de CID visées par le secret bancaire, le respect de cet accord est également garanti sur le plan pénal au travers de l'art. 47 al. 1 et 2 LB.

8 Sur la base de ce qui précède, il convient donc d'apporter la réponse suivante à la question topique:

> *Une banque suisse ne viole pas le secret bancaire au sens de l'art. 47 al. 1 et 2 de la Loi fédérale sur les banques et les caisses d'épargne (LB) lorsqu'elle transmet, dans le cadre de l'exécution d'un mandat, des données bancaires à un destinataire à l'étranger, pour autant que :*
>
> *(a) le recourt à un auxiliaire réponde à un intérêt raisonnable de la banque qui externalise, que l'auxiliaire soutienne l'activité commerciale de la banque en étant soumis aux instructions de cette dernière, et que la banque – dans l'ensemble – continue de fournir elle-même de manière prépondérante les services convenus avec le client ; et*
>
> *(b) il ne résulte d'aucun accord exprès ou tacite avec le client que le recours à un auxiliaire est interdit.*

9 La divulgation de CID dans le cadre d'une externalisation respectant les conditions susmentionnées ne constitue ainsi pas une révélation illicite au sens de l'art. 47 al. 1 LB, et ce même si le sous-traitant est situé à l'étranger et peut accéder aux données dans le cadre de son activité.

10 Une révélation punissable sous l'angle de l'art. 47 al. 1 LB ne peut être admise que lorsqu'un tiers *non autorisé* a connaissance de CID. Une telle révélation n'est toutefois soumise au droit suisse que si elle se produit en Suisse. L'art. 47 LB ne prévoyant, en outre, aucune responsabilité causale, il ne peut être invoqué qu'en présence d'une faute intentionnelle ou d'une négligence de la banque, à savoir lorsque cette dernière ne prend pas les mesures de sécurité nécessaires et, partant, cause la révélation ou contribue à celle-ci. La banque doit, par conséquent, faire preuve de la diligence commandée par les circonstances, pour ne pas se voir reprocher un comportement négligent, également sous l'angle pénal.

11 La banque n'est évidemment pas tenue dans ce contexte d'exclure toute possibilité de divulgation. Seule la création d'un risque *non autorisé* constitue une négligence. La négligence doit être écartée lorsque la banque a agi avec la diligence commandée par les circonstances. La diligence attendue de la banque

est concrétisée avant tout par la loi sur la protection des données applicable au cas d'espèce, les exigences de la FINMA contenues dans la Circulaire 2008/21 Risques opérationnels – Banques (Annexe 3) et le guide du préposé à la protection des données et à la transparence (PFPDT) relatif aux mesures techniques et organisationnelles de la protection des données. D'autres standards techniques doivent également être pris en compte, lorsqu'ils reflètent le développement technique actuel. Le respect du devoir de diligence présuppose, dès lors, une évaluation des risques que l'externalisation fait peser sur le client de la banque. Outre les risques généraux et/ou spécifiques à chaque prestataire impliqué dans l'externalisation, la banque doit également évaluer les risques spécifiques à l'étranger, si nécessaire. A cet égard, les éléments suivants jouent entre autres un rôle : l'emplacement où sont stockés / pourraient être stockés les CID, respectivement à partir duquel des accès aux CID sont possibles ; les risques juridiques pesant sur le prestataire de services en cas de violation du droit applicable à ce dernier ; les possibilités d'accès (en fait et en droit) par les autorités dans les juridictions concernées et les risques en résultant pour le client ; ainsi que, le cas échéant, les possibilités d'accès (par des autorités extérieures aux juridictions concernées en raison d'une externalisation spécifique (US CLOUD Act[1] par exemple).

12 Il résulte de ce qui précède qu'une banque qui externalise ne peut être tenue responsable en cas de révélation de CID à un tiers non-autorisé que lorsqu'elle n'a pas fait preuve de la diligence nécessaire dans le cadre de l'externalisation, causant ainsi une divulgation non autorisée. Le fait qu'une externalisation (en particulier à l'étranger) ou que l'octroi d'un accès à un auxiliaire augmente abstraitement le risque d'un accès non-autorisé ne suffit pas en soi à justifier une négligence de la part de la banque.

3. Fondements

13 L'article 47 LB prévoit ce qui suit :

> *[1] Est puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire celui qui, intentionnellement:*

[1] Clarifying Lawful Overseas Use of Data Act, Pub.L. 115–141, www.govinfo.gov/content/pkg/BILLS-115hr1625enr/html/BILLS-115hr1625enr.htm.

*a. révèle un secret à lui confié ou dont il a eu connaissance en sa qualité d'organe, d'employé, de mandataire ou de liquidateur d'une banque ou d'une personne au sens de l'art. 1*b*, ou encore d'organe ou d'employé d'une société d'audit;*

b. incite autrui à violer le secret professionnel;

c. révèle un secret qui lui a été confié au sens de la let. a ou exploite ce secret à son profit ou au profit d'un tiers.

[1bis] Est puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire celui qui obtient pour lui-même ou pour un tiers un avantage pécuniaire en agissant selon l'al. 1, let. a ou c.

[2] Si l'auteur agit par négligence, il est puni d'une amende de 250 000 francs au plus.

[3] …

[4] La violation du secret professionnel demeure punissable alors même que la charge, l'emploi ou l'exercice de la profession a pris fin.

[5] Les dispositions de la législation fédérale et cantonale sur l'obligation de renseigner l'autorité et de témoigner en justice sont réservées.

[6] La poursuite et le jugement des infractions réprimées par la présente disposition incombent aux cantons. Les dispositions générales du code pénal sont applicables.

3.1. Protection du secret bancaire

14 Le fondement juridique du secret bancaire est important pour la suite de ce rapport. Deux concepts doivent être distingués dans ce contexte :

(a) Le secret bancaire protège pénalement l'obligation de secret que la banque a envers ses clients sous l'angle du droit privé (protection individuelle) ;

(b) Le secret bancaire sert avant tout l'intérêt public dans une place financière performante, la protection des données des clients de banques en constituant le pilier central (protection systémique ou fonctionnelle).

15 Cette distinction a un impact sur la faculté des clients des banques à disposer du secret bancaire, ainsi que sur les attentes de ces derniers. Alors que, dans le premier cas, une banque peut conditionner l'établissement de relations d'affaires à la renonciation du client au secret bancaire, la liberté contractuelle est limitée par l'intérêt public dans le second cas. L'analyse du risque est également différente dans le contexte de l'externalisation. Dans le cas d'une protection individuelle, les exigences du client à l'égard de la conduite des affaires de la banque ainsi que les effets négatifs d'une violation du secret sur ce dernier constituent des éléments essentiels, alors que dans le cas d'une protection systémique, les effets négatifs sur la place financière suisse doivent être considérés avant tout.

16 Sur le plan conceptuel, l'opinion majoritaire soutient que le secret bancaire protège l'obligation de maintenir le secret professionnel découlant du droit privé (i.e. du droit contractuel et du droit de la protection de la personnalité).[2] Selon l'opinion majoritaire, l'art. 47 al. 1 et 2 LB n'a pas d'autre portée matérielle que les obligations de confidentialité visées par l'art. 398 al. 1 CO en lien avec les art. 321 al. 4 CO et 28 du Code civil suisse (**CC**).

17 Nous sommes d'avis que cette opinion est correcte. Elle s'appuie, d'ailleurs, sur les développements contenus dans le Message de 1970 concernant la révision de la loi sur les banques :[3]

> *Avant même l'entrée en vigueur de cette loi, le Tribunal fédéral avait émis l'avis que le devoir d'observer le secret constituait un élément naturel des relations contractuelles unissant la banque à ses clients. Son abandon équivaudrait à une violation des obligations*

---

2 BSK BankG-*Stratenwerth*, art. 47 no. 1; *Kleiner/Schwob/Winzeler*, Kommentar zum Bundesgesetz über die Banken und Sparkassen, Ausgabe Juli 2015, art. 47 no. 3 ss.; *Bühler*, Vom Bankgeheimnis zum automatischen Informationsaustausch, in: Breitenmoser/Ehrenzeller (ed.), Aktuelle Fragen der internationalen Amts- und Rechtshilfe, 2017, 7; *Winzeler*, Das Schweizer Bankkundengeheimnis im Wandel – Totgesagte leben länger, SJZ 2011, 98; *Althaus Stämpfli*, Kundendaten von Banken und Finanzdienstleistern, 2009, 47; *Margiotta*, Das Bankgeheimnis – Rechtliche Schranke eines bankkonzerninternen Informationsflusses?, 2002, 60; *Rappo*, Le secret bancaire, 2002, Rz. 192, 697; *Brändli*, Outsourcing, 2001, Rz. 453 f.; *Honegger/Frick*, Das Bankgeheimnis im Konzern und bei Übernahmen, SZW 1996, 2; *Fellmann*, Berner Kommentar, Bd. VI/2/4, Der einfache Auftrag, art. 394-406 OR, 1992, art. 398 OR no. 53.

3 Message du Conseil fédéral à l'Assemblée fédérale concernant la révision de la loi sur les banques , FF 1970 I 1175.

> *contractuelles en même temps qu'il constituerait une atteinte au droit qu'à la clientèle au respect du secret en tant que celui-ci est une émanation des droits assurant la protection de la personnalité. Le secret des banques découle par conséquent des dispositions générales du code des obligations sur le contrat, de même que des articles 27 et 28 du code civil, qui consacrent le principe de la protection de la personnalité.*

18 Le Message relatif à l'Initiative sur les banques de 1982 va, d'ailleurs, également dans la même direction, bien que de manière moins évidente.[4] En 2012, le Conseil fédéral a également indiqué à ce sujet que le secret bancaire est fondé sur le droit privé :[5]

> *Le secret bancaire trouve son origine dans le droit privé. […] En outre, avec l'art. 47 de la loi sur les banques du 8 novembre 1934 […], le législateur a octroyé aux clients bancaires une protection pénale supplémentaire en ce qui concerne l'obligation de garder le secret sur la relation bancaire. Cette disposition pénale ne protège cependant le secret bancaire que dans la mesure où il a été concrètement fondé par le contrat et le droit de la personnalité.*

19 Il est néanmoins, possible de trouver certaines affirmations qui peuvent être interprétées comme des allusions au concept de protection systémique. Tel est par exemple le cas dans le Message de 1934 concernant le projet de loi sur les banques:[6]

> *L'activité bancaire est si délicate et si diverse qu'on ne saurait songer à confier le contrôle à l'Etat. Le contrôle officiel n'est d'ailleurs ni dans l'intérêt de l'Etat ni dans celui des banques […] L'intervention de contrôleurs fé-*

---

4 Message sur l'initiative populaire « contre l'abus du secret bancaire et de la puissance des banques » (Initiatives sur les banques) du 18 août 1982, FF 1982 II 1237.

5 Rapport du Conseil fédéral « Les autorités sous la pression de la crise financière et de la transmission de données clients d'UBS aux Etats-Unis », en réponse au postulat 10.3390 CdG CN / 10.3629 CdG CE du 30 mai 2010, 10 octobre 2012.

6 Message du Conseil fédéral à l'Assemblée fédérale concernant le projet de loi fédérale sur les banques et les caisses d'épargne du 2 février 1934 (FF 1934 I 180).

> *déraux aurait d'autres inconvénients encore: elle inquiéterait la clientèle, qui attache une grande importance au secret bancaire et compte sur celui-ci. La fuite des capitaux déposés dans nos banques, qui serait probablement la conséquence du contrôle officiel, causerait à notre pays un préjudice dont nous devons le préserver.*

20 Dans le cadre du renforcement de l'art. 47 LB proposé par le Parti libéral-radical, lequel est entré en vigueur le 1er juillet 2015 avec la loi fédérale du 12 décembre 2014 relative à l'extension de la punissabilité en matière de violation du secret professionnel, l'intérêt public a alors clairement été mis en avant. Dans son avis du 13 Août 2014 sur le rapport de la commission compétente, le Conseil fédéral a indiqué ce qui suit:[7]

> *La violation du secret bancaire par un dépositaire dudit secret ainsi que l'utilisation et la transmission par des tiers de données bancaires acquises illégalement constituent une atteinte aux droits de la personnalité des clients des banques. De tels comportements peuvent, en outre, ébranler la confiance des clients suisses et étrangers dans la banque concernée et la place financière suisse, ce qui est susceptible de se répercuter négativement sur la compétitivité de notre place financière et sur l'économie du pays.*

21 Le Tribunal fédéral ne s'est pas encore clairement prononcé sur la question. Certaines affirmations peuvent, cependant, être comprises comme des indices en faveur d'une protection systémique. Le Tribunal fédéral a ainsi indiqué ce qui suit dans l'ATF 141 IV 155, c. 4.2.5 (bien que cet arrêt portait sur la problématique de la protection des secrets d'affaires de la banque, laquelle ne relève pas du secret bancaire) :

> *Durch die Übergabe von Daten zahlreicher ausländischer Kunden einer schweizerischen Bank an ausländische Behörden werden nicht nur die Geschäftsgeheimnisse der Kunden, sondern auch die Geschäftsgeheimnisse der Bank betroffen. Das Bank-*

[7] Initiative parlementaire « Réprimer durement la vente de données bancaires », Rapport de la Commission de l'économie et des redevances du Conseil national du 19 mai 2014 – Avis du Conseil fédéral du 13 août 2014, FF 2014 6007.

> *kundengeheimnis, welches Art. 47 des Bankengesetzes […] strafrechtlich schützt, dient nicht nur dem einzelnen Bankkunden. Es hat vielmehr auch institutionelle Bedeutung und schützt die kollektiven Interessen des schweizerischen Finanzplatzes. Diese Interessen werden betroffen, wenn Daten zahlreicher Kunden verraten werden […].*

22 Dans plusieurs décisions ultérieures en matière d'entraide judiciaire internationale,[8] le Tribunal fédéral a considéré que des intérêts essentiels de la Suisse au sens de l'ancien art. 1 al. 2 et actuel art. 1a EIMP étaient susceptibles d'être affectés :

> *[…] wenn es sich bei der vom ausländischen Staat verlangten Auskunft um eine solche handelt, deren Preisgabe das Bankgeheimnis geradezu aushöhlen oder der ganzen schweizerischen Wirtschaft Schaden zufügen würde.*

23 Dans le cadre de l'art. 273 CP, le Tribunal fédéral a également souligné en 1985 la portée systémique de la confiance dans la banque :[9]

> *Les relations entre les banques et leurs clients dépendent dans une large mesure de la confiance de ces derniers dans la discrétion dont la banque fera preuve à l'égard des faits touchant à la sphère privée du client. Si disparaît la garantie que de tels faits, révélés ou appris, resteront secrets, disparaît du même coup la confiance à cet égard du client envers la banque, et s'effondre ainsi l'une des conditions essentielles d'une activité bancaire viable.*

24 Dans une décision de 2010, le Tribunal administratif fédéral a, en revanche, clairement interprété le secret bancaire comme un devoir de protection individuel :[10]

---

8 Arrêt 1A.234/2005 du 31 janvier 2015, c. 4 ; ainsi que ATF 123 II 153, c. 7.b ; ATF 115 Ib 68, c. 4.b.

9 ATF 111 IV 74, c. 4.c.

10 Arrêt B-1092/2009 du 5 janvier 2010, c. 4.2.1.

> *Neben der privatrechtlichen Schadenersatzpflicht der Bank soll die Privatsphäre des Bankkunden im Verkehr mit der Bank auch dadurch sicher-gestellt werden, dass sich mit der Behandlung von Bankkundendaten Betraute strafrechtlich verantworten müssen, wenn sie gegen ihre Geheimhaltungspflichten verstossen. In Bezug auf Bankkundendaten ergibt sich die strafrechtliche Verantwortlichkeit nicht aus dem Berufsgeheimnis gemäss Art. 321 [StGB], sondern aus der Spezialbestimmung von Art. 47 BankG. Es handelt sich hierbei um das strafrechtliche Pendant zu Art. 398 OR […].*

25 Certains auteurs, sur la base du Message de 1934 et de la jurisprudence susmentionnée, considère que l'art. 47 LB vise, en particulier la place financière.[11] *Kunz/Zollinger* ont récemment défendu cette position, en faisant valoir que l'art. 47 LB est plus strict à certains égards que l'art. 321 CP. La violation de l'art. 47 LB constitue ainsi une infraction poursuivie d'office qui est punissable même en cas de négligence ; la diffusion et la tentative de diffusion étant – elles aussi - passibles de sanctions.[1]

26 À notre avis, les arguments selon lesquels le secret bancaire viserait également à assurer une protection systémique n'ont pas suffisamment de poids pour écarter l'opinion majoritaire. Le renforcement de la protection par rapport à l'art. 321 CP ne permet, en particulier, pas de conclure que l'art. 47 LB vise une protection systémique :

(a) La poursuite d'office de la violation de l'article 47 LB peut s'expliquer par le fait que les clients étrangers des banques pourraient ne pas être en

---

11 Emmenegger/Zbinden, Die Standards zur Aufhebung des Bankgeheimnisses, in: Emmenegger (ed.), Cross-Border Banking, 2009, 207 f. „[…] Zudem – und atypisch für das Strafrecht – dient Art. 47 BankG auch dem Funktionsschutz in Gestalt eines öffentlichen Interesses an einem attraktiven Finanzplatz Schweiz"; Heine, Die Verletzung des Bankgeheimnisses: neue Strafbarkeitsrisiken der Bank bei grenzüberschreitenden Sachverhalten, in: Emmenegger (ed.), Cross-Border Banking, 2009, 176 f. („Art. 47 BankG beschränkt sich aber nicht auf diesen Schutz individueller Interessen […] Es geht folglich um den Schutz der Institution Bankgeheimnis in ihrer Bedeutung für den Finanzplatz Schweiz"); Berger, Outsourcing vs. Geheimnisschutz im Bankgeschäft, recht 2000, 185 f. („Daraus erhellt, dass das geschützte Rechtsgut des Art. 47 BankG in Wahrheit primär der Funktionsschutz ist"); Graf, Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext, SJZ 2016, 194, ohne Begründung oder Nachweise („Art. 47 BankG [schützt] die Interessen der Bankkunden bzw. des schweizerischen Finanzplatzes"); Tissot-dit-Sanfin, Beschränkung von grenzüberschreitenden Datenflüssen im Bankbereich, 1991, 56, ohne Begründung und Nachweise („in einem untergeordneten Rahmen wird auch der Schutz der Wirtschaft […] bezweckt").

12 Kunz/Zollinger, Der Schutzbereich von Art. 47 BankG, Jusletter v. 16 April 2018, N. 8 ss.

mesure de respecter le court délai de plainte.[13] Le renforcement de la protection se justifie donc, de manière générale, par le fait qu'il convient de lutter contre les menaces spécifiques qui pèsent sur le domaine secret des clients bancaires– secret toujours fondé sur le droit privé -, telles que le commerce de données volées.

(b) Dans d'autres domaines également, la sphère privée est de plus en plus protégée pénalement, y compris par exemple dans le règlement européen sur la protection des données et, selon la volonté du Conseil fédéral, dans la future loi sur la protection des données. Ce renforcement de la protection se justifie ici aussi non pas par un besoin de protection systémique, mais par des menaces toujours plus importantes à l'encontre de la vie privée et un besoin de dissuasion.

27 Il n'apparait, en outre, pas clairement à la lecture de la jurisprudence susmentionnée que le secret bancaire vise une protection systémique. Il est évidemment vrai qu'une érosion du secret bancaire serait susceptible de porter préjudice à l'économie (voir para. N 21 ci-dessus). Cela ne permet néanmoins pas de conclure que le secret bancaire vise une protection systémique. Bien qu'il y ait évidemment un intérêt public à ne pas compromettre les institutions juridiques suisses, cela ne dit rien sur le but de protection de l'institution juridique menacée. Les décisions relatives à l'entraide judiciaire doivent également être comprises dans le même sens (voir para. N 22 ci-dessus). Ici aussi, il s'agit probablement davantage d'une question d'intérêt fondamental à la protection institutionnelle que d'un objectif de protection poursuivi par le secret bancaire. Le renforcement du régime de sanctions de l'art. 47 LB par la création de la Loi sur l'Autorité fédérale de surveillance des marchés financiers (**LFINMA**) ne permet enfin pas de conclure à l'existence d'une protection systémique. L'aggravation des sanctions visait, certes, sans aucun doute à protéger le système, les créanciers et les investisseurs.[14] Le renforcement du régime de sanctions prévu à l'art. 47 LB n'est, toutefois, probablement dû qu'à une volonté d'uniformisation.[15] Il est indéniable qu'une protection individuelle assure toujours une protection systémique. Il convient toutefois de noter, à cet égard, que tous les avis qui reconnaissent un caractère systémique au secret bancaire

[13] Ainsi Kleiner/Schwob/Winzeler, art. 47 BankG no. 2; Kunz/Zollinger, no. 11.

[14] Message concernant la loi fédérale sur l'Autorité fédérale de surveillance des marchés financiers (Loi sur la surveillance, LFINMA)

[15] Voir également le Message concernant la LFINMA, 2760 : *« Le présent projet propose donc un nouveau système consolidé et harmonisé qui comporte des sanctions pénales révisées et de nouvelles sanctions administratives. Les dispositions pénales y gagnent en substance et en uniformité, tandis que le cadre pénal est relevé ».*

ont à l'esprit le risque d'une violation *massive* du secret bancaire. Dans cette logique, les obligations de diligence et de contrôle qui incombent aux banques en vertu du principe 9 de l'annexe 3 de la Circulaire FINMA 2008/21 – Risques opérationnels – banques (**Circulaire FINMA 2008/21**) concernant l'externalisation d'activités et de prestations de services à grande échelle traitant des CID doivent être *impérativement* appliquées à toute activité impliquant un accès à *de grandes quantités de CID*.[16] Le secret bancaire n'est, toutefois, pas seulement destiné à sanctionner les violations du secret de grande importance, mais bien chaque cas individuel. Nous continuons, dès lors, à penser que l'opinion majoritaire est correcte.

3.2. La notion de secret de l'article 47 LB

28 L'article 47 LB ne consacre pas une notion indépendante de secret mais se réfère en principe – avec des limitations toutefois (voir ci-dessous) – à la conception uniforme de secret en droit pénal.[17] Un secret présuppose ainsi de manière cumulative ce qui suit:[18]

(a) *Une information inconnue du public* : seules des informations relativement inconnues peuvent être secrètes, à savoir des informations qui ne sont ni évidentes ni accessibles à tous ;

(b) *Une volonté de secret* : le titulaire du secret doit avoir la volonté de limiter la connaissance du secret à un cercle restreint de personnes. Cette volonté de secret doit en outre être perceptible, étant précisé que ceci peut également être déduit des circonstances ; et

(c) *Un intérêt au secret* : le fait de maintenir l'information secrète se fonde, conformément à des critères objectifs, sur un intérêt légitime du maître du secret.

29 Le troisième élément ci-dessus ne s'applique toutefois pas sans réserve dans le cadre de l'art. 47 LB. Dans la mesure où le secret bancaire est fondé sur le droit

[16] Circulaire FINMA 2008/21, annexe 3, para. 47. La notion de "grandes quantités de CID " doit être comprise ici comme une quantité de CID significative par rapport au nombre total de comptes / la taille totale du portefeuille de clients privés.

[17] BSK BankG-*Stratenwerth*, art. 47 no. 12 ; *Schwarz*, Geheimnisschutz- und Spionagestrafrecht, in: Jürg-Beat Ackermann/Günter Heine (ed.), Wirtschaftsrecht der Schweiz, § 19 no. 34 et 72.

[18] *Schwarz*, § 19 no. 35.

privé (voir para. N 14 ss. ci-dessus) et que le droit privé n'est pas destiné à protéger des secrets objectifs, mais plutôt le secret de manière générale,[19] il n'est pas fondamental de déterminer ce qui a le mérite de rester objectivement secret. Le seul facteur décisif dans le contexte du secret bancaire est, donc, l'intérêt du client à garder le secret, pour autant que l'invocation du secret ne soit pas exceptionnellement constitutive d'un abus de droit.[20]

30 Les informations anonymes, à savoir les informations qui ne peuvent pas être rattachées à une personne physique ou morale déterminée, ne sont pas protégées par l'art. 47 LB.[21] Sous l'angle du droit suisse, il convient donc se rapporter aux critères de la protection des données pour ce qui concerne les références aux personnes. Les données des clients d'une banque comprennent donc toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3 LPD), étant précisé que le Tribunal fédéral définit le critère d'identifiabilité comme suit:[22]

> *Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor […]. Die Frage ist abhängig vom konkreten Fall zu beantworten, wobei insbesondere auch die Möglichkeiten der Technik mitzuberücksichtigen sind, so zum Beispiel die im Internet verfügbaren Suchwerkzeuge. Von Bedeutung ist indessen nicht nur, welcher Aufwand objektiv erforderlich ist, um eine bestimmte Information einer Person zuordnen zu können, sondern auch, welches Interesse der Datenbearbeiter oder ein Dritter an der Identifizierung hat […].*

---

19 Voir par exemple *Fellmann*, art. 398 no. 53 (*„[…] Bei der vertraglichen Schweigepflicht geht es demgegenüber […] nicht primär um die Wahrung, von Geheimnissen, sondern generell um Verschwiegenheit […]. Entscheidend ist hier nicht, was objektiv geheimhaltungswürdig ist; massgebend ist vielmehr allein das Geheimhaltungsinteresse des Auftrag-gebers, wie es für den Beauftragten erkennbar war bzw. nach den Umständen erkennbar sein musste"*).

20 *Margiotta*, 38; *Michlig*, Bankgeheimnisverletzung (Art. 47 BankG) unter dem Aspekt der Lieferung von Personendaten ans U.S. Department of Justice, AJP 2014, 1059.

21 Voir arrêt du *Handelsgericht* de Zurich HG150170 du 30 mai 2017, c. 5.3.5.1.

22 ATF 136 II 508 – Logistep, c. 3.2.

31 Les informations sont donc anonymes lorsque, compte tenu de l'ensemble des circonstances, en particulier des possibilités techniques et de l'intérêt à prendre connaissance des informations soumises au secret bancaire, la possibilité d'en prendre connaissance n'est pas envisageable selon l'expérience générale de la vie.[23] Il n'est ainsi pas possible de conclure à une divulgation de CID lorsqu'il est impossible d'en prendre connaissance, à savoir notamment lorsque les informations sont anonymisées, pseudonymisées ou chiffrées, de telle sorte que le destinataire ne puisse les rattacher à une personne (voir para. N 41 du Guide ; cf. également Circulaire FINMA 2008/21, annexe 3, para. N 65).

3.3. La notion de révélation

32 L'art. 47 de la LB interdit la « révélation » d'un secret qui a été confié ou dont la nature secrète est reconnue. Ce même article ne définit toutefois pas la notion de révélation. Il faut donc supposer qu'il existe un concept général de révélation en droit pénal. La révélation se rapporte toujours à un tiers non autorisé, à savoir une personne différente du maître du secret, de son titulaire ou de ses employés et auxiliaires[24] (en ce qui concerne les auxiliaires, voir para. n° 47 ss. ci-dessous), comme cela découle sans autres précisions du texte de l'art. 47 al. 1 let. a LB.

33 Conformément à la jurisprudence applicable jusqu'à présent,[25] le seul fait de permettre à un tiers de pouvoir prendre connaissance d'une information était

---

[23] Voir, à ce sujet, arrêt du Handelsgericht de Zurich HG150170 du 30 mai 2017, c. 5.3.5.2 („Anonymisierung bedeutet, dass der Personenbezug irreversibel so aufgehoben wird, dass ohne unverhältnismässigen Aufwand keine Rückschlüsse auf Personen mehr möglich sind. Anders als bei der Pseudonymisierung darf kein Schlüssel (Zuordnungsregel) aufbewahrt werden, der die Re-Identifikation der betroffenen Person ermöglicht. Um eine Re-Identifikation auszuschliessen, reicht es vielfach nicht aus, klar identifizierende Merkmale wie Vorname, Name, Geburtsdatum und Adresse zu entfernen. Bei einer Pseudonymisierung soll der Personenbezug aufgehoben werden, aber bloss reversibel. Der Schlüssel zur Re-Personifizierung der Informationen bleibt erhalten. Deshalb bleiben pseudonymisierte Personendaten für alle, die Zugang zum Schlüssel haben, weiterhin Personendaten. Einzig für Aussenstehende, welche die pseudonymisierten Daten ohne Schlüssel ausgehändigt erhalten haben und die konkret auch keinen Zugang zum Schlüssel haben, sind pseudonymisierte Personendaten wie anonymisierte keine Personendaten mehr.").

[24] Voir Schwarz, § 19 no. 77 s. („Entscheidend ist also, dass vom Bankgeheimnis geschützte Informationen an Aussenstehende offenbart werden. Dies bietet keine Probleme, wenn der Geheimnisträger Informationen an weder mit der Bank noch mit dem Kunden in irgendeiner Art verbundene Dritte oder gar an die Öffentlichkeit gibt").

[25] A ce sujet, arrêt du Tribunal pénal fédéral du 10 décembre 2013, SK. 2013.37, c. 3.2.1 concernant les art. 321 et 162 CP („Umstritten ist, ob die Tat bereits mit der Einräumung der Möglichkeit der Kenntnisnahme des Geheimnisses an Dritte vollendet wird […] oder erst mit der Kenntnisnahme durch den Geheimnisempfänger […]. […] Aufschlussreich ist indessen die bundesgerichtliche Rechtsprechung zu Art. 321 StGB […]. […] Laut Bundesgericht umfasst der Begriff des Offenbarens im Sinne von Art. 321 StGB jede Art der Bekanntgabe des Geheimnisses, insbesondere auch die

considéré comme une révélation, sans qu'une prise de connaissance effective par le tiers ne soit nécessaire. Dans l'arrêt 6B_1403/2017, le Tribunal fédéral s'est toutefois expressément écarté de cette jurisprudence, en considérant qu'une prise de connaissance effective par le tiers était nécessaire:[26]

> *Nach Art. 162 StGB macht sich unter anderem strafbar, wer ein Fabrikations- oder Geschäftsgeheimnis, das er infolge einer gesetzlichen oder vertraglichen Pflicht bewahren sollte, verrät. Die Tathandlung ist dieselbe wie bei den Tatbeständen der Verletzung des Amtsgeheimnisses (Art. 320 StGB) oder des Berufsgeheimnisses (Art. 321 StGB). In dem von der Vorinstanz erwähnten BGE 142 IV 65 E. 5.1 hat das Bundesgericht erwogen, dass ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme ermöglicht. Es handelt sich hierbei um eine blosse Umschreibung des strafbaren Verhaltens, woraus – entgegen der Meinung der Vorinstanz – nichts zum Zeitpunkt der Vollendung der Tat abgeleitet werden kann.* ***Vielmehr ist in dieser Frage der Lehre zu folgen, wonach die Tat vollendet ist, sobald ein Aussenstehender dank dem Verhalten des Täters Kenntnis vom betreffenden Geheimnis erhält.*** *Strafbarer Versuch wäre insbesondere dann anzunehmen, wenn der Täter Informationen für einen Dritten zugänglich gemacht hat, dieser aber vom Geheimnis noch keine Kenntnis genommen hat […]. Keiner der Mitarbeiter der B. Sagl nahm von den Zeichnungen, welche sich im Altpapier befanden, Kenntnis. Ein Schuldspruch wegen einer vollendeten Verletzung des Fabrikations- oder Geschäftsgeheimnisses ist damit von vornherein ausgeschlossen.*

Aushändigung von Schriftstücken oder anderen Sachen, die das Geheimnis verraten […]. Eine Kenntnisnahme des Geheimnisses durch den Empfänger ist demnach für die Tatvollendung im Rahmen von Art. 321 StGB nicht erforderlich. Für Art. 162 al. 1 StGB kann nichts anderes gelten"); confirmé, entre autres, par le Tribunal pénal fédéral dans un arrêt du 4 avril 2018, SK.2017.52; voir aussi ATF 142 IV 65, c. 5.1 („Ein Geheimnis offenbart, wer es einer dazu nicht ermächtigten Drittperson zur Kenntnis bringt oder dieser die Kenntnisnahme zumindest ermöglicht").

[26] Arrêt 6B_1403/2017 du 8 août 2017, c. 1.2.2, SJZ 2018, 453.

34 Si l'on applique cette jurisprudence à l'art. 47 al. 1 et 2 LB, il en découle par exemple qu'un stockage négligeant de données ne suffit pas pour constituer une révélation, tant et aussi longtemps que le manque de diligence ne conduit pas à la prise de connaissance effective des données par une personne non autorisée. *Schwarzenegger, Thouvenin, Stiller* et *George* arrivent également à cette conclusion sur la base de leur rapport d'experts concernant l'utilisation de services « cloud » par des avocat(e)s.[27] Sur la base de l'arrêt précité, les auteurs susmentionnés arrivent d'ailleurs même à la conclusion que l'art. 321 CP constitue une infraction matérielle et non formelle.

35 La doctrine traditionnelle est majoritairement d'avis que la simple possibilité d'une prise de connaissance suffit.[28] La jurisprudence antérieure s'exprimait d'ailleurs également dans ce sens, comme l'a par exemple exprimé l'*Obergericht* de Zurich dans un arrêt de 2017 :[29]

> *[g]eheimzuhaltende Tatsachen zu offenbaren, bedeutet sodann, sie Unberufenen zugänglich zu machen.*

36 Le Tribunal pénal fédéral a également statué dans le même sens en 2013.[30]

37 Ces arrêts et avis de doctrine sont toutefois plus anciens que l'arrêt du Tribunal fédéral précité. Rien ne laisse, de surcroît, penser que l'acte de révélation pénalement répréhensible varie en fonction du secret concerné. Il faut plutôt supposer que la notion de révélation est uniforme. Une révélation au sens de l'art. 47 al. 1 et 2 LB ne peut donc être reconnue qu'en cas de prise de connaissance effective d'un secret par un tiers non autorisé. Une divulgation de données intentionnelle ou par dol éventuel sans prise de connaissance constitue donc tout au plus une tentative pénalement répréhensible en application des art. 22 et 333 CP (à ce sujet, voir également para. N 39 s.).[31]

---

27 Voir *Schwarzenegger/Thouvenin/Stiller/ George,* Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, AnwaltsRevue 2019, 25 ss. Cet avis d'experts a été publié au nom de la Fédération Suisse des Avocats en novembre 2018. Il n'a pas encore été publié, mais est mis à disposition des auteurs et sera publié dans la collection du *Center for Information Technology, Society, and Law (ITSL)* de l'Université de Zurich.

28 Voir, par exemple, BSK-*Stratenwerth*, art. 47 no. 15; *Schwarz*, § 19 Rz. 76; *Jositsch*/*Conte*, Bankgeheimnisverletzung durch Whistleblowing, SJZ 2017, 360; *Stratenwerth*/*Bommer*, Schweizerisches Strafrecht BT II, 7. ed. 2013, § 61 no. 7 et 19 („nach allgemeiner Auffassung"); ***contra*** (pour lesquels une prise de connaissance est nécessaire) *Dupuis, Moreillon et al.*, Petit Commentaire Code Pénal, 2. ed. 2017, art. 320 CP no. 29 et art. 321 CP no. 33.

29 Arrêt SB160259 du 16 août 2017, c. 6.1.1.

30 Arrêt SK.2013.37 du 10 décembre 2013, c. 3.3.2 c, forumpoenale 6/2014, 332 (la remise d'un support de données suffit).

31 A ce sujet, BSK-*Niggli/Maeder*, art. 22 CP no. 2.

38 A titre de conclusion intermédiaire, l'on doit donc admettre que :

(a) une divulgation autorisée de CID (p. ex. à un auxiliaire autorisé) ne constitue pas une révélation sous l'angle pénal, et ce même si l'auxiliaire se trouve à l'étranger;

(b) une divulgation de CID ne constitue pas non plus une révélation pénalement répréhensible, lorsque les données concernées ne permettent pas au destinataire de faire un lien avec des personnes spécifiques, par exemple parce que les CID ont été anonymisées ou pseudonymisées de telle sorte que le destinataire ne peut les attribuer à personne ;

(c) pour terminer, une divulgation de CID ne constitue pas une révélation pénalement répréhensible, lorsqu'elle n'a pas pour conséquence la prise de connaissance par un tiers non autorisé des CID concernées. Ceci vaut également en cas de stockage imprudent de CID, si celui-ci reste sans conséquences. Dans ce dernier cas, toutefois, une tentative de révélation peut être admise sur le plan pénal en cas d'intention ou de dol éventuel.

3.4. Critère subjectif

39 D'un point de vue subjectif, l'art. 47 al. 1 et 2 LB exige une intention ou une négligence :

(a) lorsqu'il s'agit d'une infraction intentionnelle, l'intention doit porter sur tous les éléments objectifs de l'infraction,[32] à savoir également la prise de connaissance non autorisée des CID (voir para. N 32 ss. ci-dessus).

(b) en cas d'infraction par négligence, la violation du devoir de diligence de la banque, auquel celle-ci est tenue de part les circonstances (art. 12 al. 3 CP), doit être à l'origine de la divulgation non autorisée (pour les détails, voir para. N 65 ss. ci-dessous).

40 La divulgation de CID ne constitue, dès lors, pas une révélation pénalement répréhensible lorsque la banque n'agit pas intentionnellement ou de façon négligente, et ce même si la divulgation donne (quand même) lieu à une prise de

[32] *Donatsch/Tag*, Strafrecht I – Verbrechenslehre, 9. ed. 2013, 112.

connaissance par une personne non autorisée. Dans ce contexte, il convient d'examiner en particulier si un manquement à l'obligation de diligence peut être imputé à la banque ; en effet, même dans le cas d'une externalisation diligente, il ne peut être exclu que l'auxiliaire commette une faute. Il convient, notamment, de déterminer avec précision la personne responsable du manquement effectif à l'obligation de diligence (conformément à la répartition des rôles qui est autorisée entre la banque et l'auxiliaire), dans la mesure où seule cette personne peut avoir manqué à cette obligation et, partant, avoir agi avec négligence. En règle générale, les obligations de la banque dans ce contexte se limitent aux devoirs de sélection, d'instruction et de surveillance, lesquels doivent respecter les règles et pratiques en vigueur. Si la banque respecte ces devoirs, aucune négligence ne peut lui être reprochée lorsque l'auxiliaire viole une obligation qui lui a été déléguée.

41 Seule la création d'un risque *illicite* est, en outre, susceptible de justifier une négligence.[33] Le fait qu'une activité (telle que l'externalisation du traitement de données, par exemple) est généralement associée à des risques prévisibles pour les justiciables doit être accepté, même si les risques en question ne peuvent être exclus avec la diligence requise (à l'exception des situations où le législateur aurait interdit l'activité correspondante, ce qui n'est pas le cas en l'espèce). La seule réalisation des risques résiduels ne peut, dès lors, être reconnue comme un manquement à l'obligation de diligence.

42 Une tentative punissable de révélation n'est donc concevable qu'en présence d'une intention[34], à savoir lorsque la banque veut ou, à tout le moins, accepte dans le sens d'un dol éventuel qu'une personne non autorisée prenne connaissance des CID, mais que ce résultat ne se concrétise pas.

3.5. Punissabilité de l'infraction à l'étranger

43 En principe, le code pénal suisse est applicable aux actes commis sur le territoire suisse (art. 3 al.1 CP, principe de territorialité). Le lieu de commission de l'infraction, conformément à l'art. 8 al. 1 CP, inclut tant le lieu où l'auteur a agi ou aurait dû agir que le lieu où le résultat s'est produit (principe d'ubiquité). Le lieu où l'auteur a agi est d'abord là où se sont réalisés les éléments objectifs du comportement pénal, soit dans le cas d'une révélation non autorisée, là où la

[33] BSK-*Niggli/Maeder*, art. 12 CP no. 98.
[34] BSK-*Niggli/Maeder*, art. 22 CP no. 1 et 2.

révélation a eu lieu. Ainsi, si une banque suisse révèle des CID sans autorisation, le lieu de commission de l'infraction est la Suisse, alors que si c'est le fait d'un prestataire de services sis à l'étranger le lieu de commission se trouvera dans le pays étranger concerné.

44 Le lieu du résultat se trouve, quant à lui, à l'endroit où le résultat de l'infraction se produit.[35] Si l'on suit la jurisprudence du Tribunal fédéral selon laquelle l'infraction de violation du secret présuppose une prise de connaissance effective du secret (voir para. N 32 ss. ci-dessus), le résultat peut seulement se situer là où la prise de connaissance s'est produite, c'est-à-dire à l'endroit où le destinataire non autorisé se trouvait lorsqu'il a reçu l'information.

45 Ainsi, si la banque transmet des CID de façon non autorisée à un prestataire de services à l'étranger qui fait à son tour illégalement prendre connaissance de ces CID à un tiers se trouvant dans un pays étranger (par exemple une agence gouvernementale étrangère), le lieu où le résultat se produit peut uniquement être le pays étranger en question. Dans ce cas, la Suisse n'est ni le lieu où l'auteur a agi ni celui où le résultat s'est produit eu égard au prestataire de services. Par conséquent, le caractère pénalement répréhensible dans ce cas dépendra des conditions de l'art. 7 CP, soit de savoir si la révélation est également pénalement répréhensible sur le territoire étranger du lieu de commission.

46 Dans cette constellation, en revanche, il existe pour la banque un lieu de commission en Suisse[36] si elle a violé une obligation de diligence lui incombant (voir para. N 40 ci-dessus) et contribué de façon causale au résultat, de sorte qu'elle est exposée dans ce cas à un risque de responsabilité pénale.

4. Admissibilité de l'externalisation du traitement de données d'identification du client (CID) à un prestataire de services

47 Bien que l'art. 47 al. 1 LB ne le mentionne pas expressément, il va sans dire que seule une révélation à une personne non autorisée est pénalement répréhensible. À cet égard, la question se pose de savoir si et dans quelles circonstances un secret peut être confié à un auxiliaire.

---

35 A ce sujet *Gless*, Internationales Strafrecht, 2ème éd.. 2015, no. 149 ss.

36 Il suffit que l'infraction soit réalisée seulement en partie sur le territoire suisse. Voir à cet égard la décision 6B_86/2009 du 29 Octobre, considérant 2.3.

4.1. Admissibilité de l'externalisation à des auxiliaires

48 Il est incontestablement légal d'externaliser des CID [37] soumises au secret bancaire si cela n'entraîne pas une révélation, soit si le prestataire de services ne prend pas connaissance des CID. D'un point de vue pratique, cela n'est toutefois concevable pour des solutions de stockage que si la personne auxiliaire reçoit des données cryptées non susceptibles d'être décryptées.

49 En ce qui concerne la révélation de CID non cryptées (ou de CID cryptées auxquelles l'auxiliaire peut avoir accès de manière générale ou dans certaines circonstances), certains auteurs, en particulier *Wohlers*, considèrent que l'externalisation requiert le consentement du client concerné.[38] A cette opinion s'oppose le fait que l'implication d'une personne auxiliaire est inévitable dans de nombreuses situations et sert aussi les intérêts du client. Le point de vue défendu par Wohlers est donc impraticable. Cette opinion contredit également l'attitude du Conseil fédéral qui, il y a des décennies déjà, considérait que l'externalisation de certains services à des mandataires impliquant une révélation de CID était autorisée. Lors de la révision de la loi sur les banques en 1971, les « mandataires » de la Banque ont été inclus dans le cercle des personnes soumises au secret au sens de l'art. 47 al. 1 LB. Le Message de 1970[39] établit à ce sujet que:

> *En y soumettant les mandataires, on a voulu y englober en particulier les centres de calcul qui sont chargés par les banques du traitement électronique des informations.*

50 Il en résulte que l'externalisation du traitement de CID par des mandataires, par exemple dans le domaine de l'informatique, est en principe autorisée selon le Conseil fédéral. Dans une prise de position non publique du 21 juin 1999, l'Office fédéral de la justice est également parvenu à la conclusion que l'externalisation de la facturation et des services informatiques par les médecins est également autorisée même sans le consentement des patients.[40]

---

37 Ici le terme "externalisation" est plus ou moins utilisé comme un synonyme de "révélation".

38 *Wohlers*, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Art. 321 StGB), 2016, passim; *idem*, Outsourcing durch Berufsgeheimnisträger, digma 2016, passim.

39 Message du Conseil fédéral concernant la révision de la loi sur les banques du 13 mai 1970, FF I 1197.

40 *Casanova*, Datenverknüpfung in ausgewählten Bereichen: Gesundheitswesen, in: Epiney/Probst/Gammenthaler (ed.), Datenverknüpfung – Problematik und rechtlicher Rahmen, Zürich 2011, 48.

51 La jurisprudence considère également que l'externalisation effectuée par les banques est en principe autorisée. Dans l'arrêt BGE 121 IV 45 (considérant 2a), le Tribunal fédéral a par exemple retenu que :

> *Es entspricht einer Übung, dass auch juristische Personen mit eigenem Rechtsdienst, wie Versicherungen und Banken, Anwälte im Mandatsverhältnis beiziehen, wenn es um die Führung von Prozessen geht, nicht zuletzt deshalb, um von der forensischen Erfahrung der Anwälte zu profitieren. Dies erscheint zulässig, unter Umständen sogar geboten […].*

52 Dans une décision de 2015, l'*Obergericht* de Zurich a constaté que:[41]

> *[…] Im Urteil BGE 121 IV 45 E. 2b erachtete das Bundesgericht den Beizug von Anwälten durch eine Bank als Übung, wenn es um die Führung von Prozessen gehe. Die Bank profitiere von der forensischen Erfahrung der Anwälte, auch wenn sie über einen eigenen Rechtsdienst verfüge. Das scheine zulässig, unter Umständen sogar geboten. Daraus kann abgeleitet werden, dass der übungsgemässe Beizug von Anwälten offenbar nicht geradezu zwingend geboten sein muss, um zulässig zu sein. […]*

53 En 2016, le Tribunal cantonal de Lucerne a même indiqué ce qui suit:[42]

> *Die Ausgestaltung der Beziehung zwischen der Bank und ihren Kunden (der Kundenbeziehung) stellt auf dem Finanzdienstleistungsmarkt ein erheblicher Wettbewerbsfaktor dar. Dementsprechend haben die Banken an einer Optimierung der Kundenbeziehungen ein starkes Interesse. Letzten Endes profitieren auch die Kunden davon. Die Erforschung der Kundenbedürfnisse entspricht damit fraglos einem ernstzunehmenden Interesse der Bank D AG, was zur Folge hat, dass die Beauftragung eines professionellen Marktforschungsinstituts*

[41] Arrêt du 9 juillet 2015, Geschäfts-Nr. UE140317, cons. 6.4.

[42] Arrêt du 7 décembre 2016, LGVE 2016 I Nr. 21, c. 6.4.

– auch wenn der Kreis der Beauftragten im Sinne von Art. 47 Abs. 1 lit. a BankG eng auszulegen ist – in diesem Bereich möglich bleiben muss.

54 La jurisprudence a également considéré que l'externalisation était autorisée pour d'autres secrets professionnels. C'est ainsi que le Tribunal d'arrondissement de Zurich a estimé que le recours par un médecin à un « service central de secrétariat » était autorisé puisque ce service central de secrétariat devait être qualifié d'auxiliaire.43

55 La doctrine a également réfuté l'opinion de *Wohlers*, dans la mesure où elle a abordé le sujet.[44]

56 Sur la base de tout ce qui précède, il doit être conclu que l'externalisation est en principe autorisée et ce même si l'auxiliaire peut accéder aux données non cryptées de manière générale ou à certaines conditions. À cet égard, une réelle nécessité d'externalisation ne doit pas être exigée. Dans les cas examinés, la jurisprudence a également considéré qu'un usage en la matière ou un intérêt à optimiser la relation client était suffisant. La majorité de la doctrine estime qu'une externalisation sans le consentement du client est autorisée si elle est opportune.[45] Ces auteurs exigent, toutefois, conformément à la jurisprudence susmentionnée, que l'externalisation:

(a) « serve un véritable intérêt d'optimisation des services ou de réduction des coûts »;[46]

(b) « réponde à des motifs de division du travail et d'efficacité des coûts »,[47] comme c'est le cas par exemple lors de « l'implication de […] développeurs de logiciels. »[48]

---

43 Arrêt GG150233-L du 18 novembre 2015, c. 2.5.

44 Dans ce sens *Chappuis/Alberini*, Secret professionnel de l'avocat et solutions cloud, AnwaltsRevue 2017, 337 ss.; *Thouvenin/Schwarzenegger/Stiller/George*, 26 ss.; *Trüeb/Zobl,* Steuerdaten in der Cloud, digma 2016, 105.

45 Ainsi, BSK-Stratenwerth, article 47 LB No. 7; Stocker, Regulatorische Anforderungen an IT-Outsourcing: Finanzmarktbereich, in: Weber/Berger/Auf der Maur (ed.). IT-Outsourcing 2003, 250 f. (en raison d'une "certaine nécessité"). Autrement, Althaus Stämpfli, 224, qui exclut l'externalisation sans consentement en se plaçant sous l'angle des frais bancaires ; Berger, 191, selon qui l'intérêt de la banque à procéder à l'externalisation n'est pas suffisant en lui-même et en général il est impossible de déterminer quel intérêt de la banque à sous-traiter supplante l'intérêt du client à la protection de son secret ; Aubert/Béguin/Bernasconi/ Graziano-von Burg/Treuillaud, 103, selon qui l'externalisation est seulement permise si la banque ne peut réaliser elle-même l'activité en question, ce qui doit être admis seulement avec réserve .

46 BSK-*Stratenwerth*, art. 47 BankG no. 7.

57 Ces restrictions sont trop strictes à notre avis. Sous l'angle du droit des obligations, conformément à l'art. 68 CO, il est possible de conclure à une autorisation de principe – mais dispositive -- de l'externalisation à un auxiliaire.[49]

> *Dieser Grundsatz ist eine Voraussetzung einer arbeitsteiligen Gesellschaft; Art. 68 ist deshalb materielle Basis zahlreicher schuldrechtlicher Institute, z.B. des Wechsels und des Checks […] sowie des Arbeitsvertrages […], denn bestünde Art. 68 nicht in der vorliegenden Weise, müsste der Schuldner regelmässig persönlich leisten und dürfte die Arbeitslast nicht mittels Anstellung von Hilfskräften (Arbeitnehmer) verteilen. Art. 68 bringt insoweit einen wichtigen Beitrag zu einer – ökonomisch betrachtet – effizienteren Wirtschaft.*

58 Il en va de même pour les activités bancaires. S'il résulte de l'art. 398 al. 3 CO qu'un "transfert" (c'est-à-dire une substitution) du mandat est illicite, cela ne signifie pas pour autant que toute intervention d'un tiers est exclue. L'intervention d'auxiliaires au sens de l'art. 101 CO demeure - contrairement au transfert des obligations principales d'exécution d'un contrat (substitution) - dans une large mesure licite[2]. Ainsi par exemple, même un chirurgien qui est personnellement tenu de réaliser une opération peut faire appel à un « infirmier anesthésiste », *« tant que sa prestation demeure matériellement prépondérante»*, et *«selon les circonstances concrètes […] la supervision et le contrôle par le débiteur [suffisent]»* [51]. (Aussi) pour les banques, on peut donc supposer que l'externalisation à un auxiliaire est autorisée par le droit privé dans la mesure où:

(a) l'externalisation répond à un intérêt raisonnable de la banque qui externalise;

---

47 *Honegger/Frick*, 6; *Brändli*, N. 457.

48 *Honegger/Frick*, 6.

49 *Weber*, in: Berner Kommentar Band/Nr. VI/1/4, Die Erfüllung der Obligation, art. 68-96 OR, 2. Aufl. 2005, art. 68 OR no. 5.

50 *Bühler*, in: OFK OR, 3. Aufl. 2016, art. 398 OR no. 9; *Thionnet-Chevrier/Falletti/Bizzozero*, Le mandat de gestion de fortune, 2. Aufl. 2017, 131.

51 Ainsi BK-*Weber*, art. 68 OR no. 32.

(b) l'externalisation est comprise comme l'intervention d'un auxiliaire, à savoir que les activités de l'auxiliaire assistent les activités commerciales de la banque et sont soumises à son pouvoir de surveillance ; et

(c) la banque effectue elle-même de manière prépondérante les services convenus avec ses clients.

59 Tant que ces conditions sont remplies l'intervention en tant que telle est contractuellement autorisée (à moins qu'un contrat ne stipule le contraire) et ne viole aucunement la protection du secret sous l'angle du droit de la protection de la personnalité.[52] Il s'ensuit également que le secret bancaire renforce pénalement le devoir d'observer le secret fondé sur le droit privé (voir para. N 14 ss. ci-dessus). C'est la raison pour laquelle en droit pénal, seul l'art. 68 CO peut trouver application dans la mesure où l'article 47 al. 1 LB emploie le terme « mandataires » sans en délimiter le cercle.

60 En cas d'intervention autorisée, la banque n'est pas tenue de se faire délier du secret bancaire, au cas par cas par le biais d'un « waiver » ou de manière générale.[53] Ce n'est pas que la violation de la confidentialité est justifiée mais plutôt que les éléments d'une révélation non autorisée ne sont pas réunis.

61 Ceci est, toutefois, subordonné à la condition qu'il ne découle pas d'un accord - qu'il soit exprès ou tacite - que l'intervention n'est pas autorisée. Si un accord contractuel prévoit l'interdiction de la révélation de CID à l'étranger, le respect de cet accord est également protégé en droit pénal par l'art. 47 al. 1 et 2 LB. Dans ce cas, la révélation à l'étranger nécessite le consentement préalable du client pour le cas spécifique ("waiver") ou la modification préalable de la disposition contractuelle correspondante. Pour déterminer s'il a été convenu d'une exclusion de la révélation à l'étranger, il faut tenir compte non seulement des conventions expresses entre la banque et le client titulaire (par exemple des dispositions correspondantes des conditions générales), mais aussi de toutes les autres circonstances qui, dans leur ensemble, peuvent amener à conclure qu'il existe un engagement en ce sens de la banque (qui peut être conclu tacitement conformément à l'art. 6 CO), ainsi que le comportement de la banque

[52] Si la banque viole une disposition de la loi sur la protection des données, par exemple l'obligation de transparence, ceci pourra servir à caractériser une violation de la personnalité en vertu de l'article 12 paragraphe 1 de la LPD, mais il ne peut pas en être déduit que la divulgation à cause de l'implication d'un prestataire de service est illicite en tant que telle.

[53] Les problèmes de transparence pouvant être soulevés par la loi sur la protection des données ne rentrent pas dans le champ de cet avis de droit.

et sa situation sur le marché, les déclarations sur la protection des données et, dans une certaine mesure, la pratique professionnelle de la branche.

4.2. Admissibilité de l'externalisation à l'étranger

62 L'art. 47 LB n'interdit pas expressément l'externalisation du traitement de données dans un pays étranger. Les travaux préparatoires ne mentionnent pas non plus une quelconque responsabilité pénale. Une partie de la doctrine considère, néanmoins, que l'externalisation du traitement de CID à l'étranger entraîne, en droit (voir para. N 43 ss. ci-dessus) ou en fait, une perte de la protection pénale et que le client pourrait de ce fait, dès lors, supposer qu'une violation du secret entraîne des sanctions pénales. L'externalisation à l'étranger requerrait sur cette base, par conséquent, un consentement du client.[54]

63 Ce point de vue est corroboré par le fait que l'art. 47 al. 1 et 2 LB sanctionne les violations du secret. Le législateur a évidemment jugé nécessaire, afin de protéger les clients des banques, de menacer d'une sanction les détenteurs du secret. Ce choix législatif ne peut être considéré comme anodin, ce d'autant plus que les sanctions encourues ont encore été renforcées dernièrement (voir para. N 20 ci-dessus). Il est toutefois trop catégorique de conclure que l'externalisation par le biais d'un mandataire étranger est interdite dans tous les cas. D'une part, l'art. 47 LB ne contient aucune base claire permettant de sous-tendre une pareille interdiction, de telle sorte qu'en raison du principe de la légalité (art. 1 CP), la transmission de données à un prestataire de services à l'étranger ne peut être exclue de manière générale. D'autre part, il convient d'appliquer, lors d'une transmission de données à l'étranger, des critères identiques à ceux qui sont appliqués dans le cadre d'une externalisation à un prestataire de services en Suisse (à ce sujet, voir para. N 44 ss ci-dessus). Il faut dès lors considérer qu'il est, en principe, également possible de faire appel à un prestataire de services à l'étranger. La banque doit, dans ce contexte, respecter la diligence découlant des circonstances, ce qui soulève des questions supplémentaires lors d'une transmission de données à l'étranger (cf. para. N 65 ss.).

[54] *Brändli*, no. 480.

4.3. Conclusion

64 La banque peut transmettre des CID à un prestataire de service dans la mesure où l'intervention de ce dernier répond à un intérêt raisonnable de la banque et ne contrevient à aucun accord avec le client. Ceci vaut, en principe, également en cas de d'intervention d'un prestataire de services à l'étranger. A cet égard, il n'est pas nécessaire que les CID soient cryptées pour empêcher que le prestataire de services puisse en prendre connaissance. La banque n'est passible de sanctions en vertu de l'art. 47 al. 1 et 2 LB que:

(a) si elle révèle des CID à une personne sans le consentement du client, alors que cette personne n'est pas un mandataire, mais uniquement un tiers ; ou

(b) si elle ne prend pas les mesures nécessaires pour réduire les risques et contribue ainsi de manière causale à ce que les CID soient portées à la connaissance d'un tiers non autorisé, pour autant que la banque ait agi intentionnellement, par dol éventuel ou par négligence (voir para. N 39 et s. ci-dessus). Cette dernière problématique est approfondie dans la section suivante.

5. Critères de diligence dans le cadre de l'externalisation

65 La banque est tenue d'agir avec toute la diligence commandée par les circonstances lorsqu'elle fait appel à des auxiliaires. Si la banque ne fait pas preuve de la diligence requise et que ceci entraine de manière causale une révélation de CID par l'auxiliaire à une personne non autorisée, dont la cause est le manque de diligence, il est possible d'admettre une violation intentionnelle ou négligente de l'art. 47 al. 1 et 2 LB.[55]

66 Ceci soulève la question de savoir quelle diligence est « commandée par les circonstances » (art. 12 al. 3 CP). Le juge pénal y répondra dans chaque affaire de façon discrétionnaire, si bien que le danger existe qu'une divulgation non autorisée soit automatiquement reconnue comme une violation du devoir de diligence, et ce même si cette position est évidemment inadmissible.

[55] D'autres obligations de la banque découlent, le cas échéant, d'autres dispositions relatives à la protection du secret, telles que les art. 162 ou 273 CP ainsi que du droit applicable en matière de protection des données.

67 Il est également important de relever qu'il convient, sous l'angle pénal, de déterminer à chaque fois qui est affecté par la violation du devoir de diligence et si un risque non autorisé a été créé (voir para. N 40 ci-dessus).

68 La concrétisation du devoir de diligence passe avant tout par l'application des règles légales de diligence raisonnable dans le domaine en question. Revêtent également une importance particulière les recommandations, lignes directrices, brochures et autres documents généralement reconnus, émis par des organismes privés ou publics[56]. L'ensemble des règles suivantes (sans être exhaustif) sont, dès lors, susceptibles de faire autorité :

(a) les exigences de la loi suisse sur la protection des données relatives à la sécurité des données (voir art. 7 LPD et art. 8 ss. de l'ordonnance relative à la loi fédérale sur la protection des données, **OLPD**), qui requiert le respect du « développement technique » (art. 8 al. 2 let. d OLPD).

(b) le cas échéant, les exigences de la loi suisse sur la protection des données concernant le transfert de données personnelles à l'étranger (art. 6 LPD et 5 ss. OLPD).

(c) les exigences de l'annexe 3 de la Circulaire FINMA-RS 2008/21 (Traitement des données électroniques de clients).

(d) le guide du Préposé fédéral à la protection des données et à la transparence relatif aux mesures techniques et organisationnelles de la protection des données, dans la mesure où il contient des recommandations sur l'utilisation de certaines mesures techniques et organisationnelles (**MTOs**).

(e) le cas échéant, d'autres standards techniques pertinents, lorsque ceux-ci reflètent le développement technique actuel.

69 Ces règles exigent au préalable une évaluation des risques associés à l'externalisation. A cet égard, la banque doit en règle générale apprécier les points suivants :

(a) les risques pour la sécurité des données existant dans le cas d'espèce, y compris l'effet des mesures d'atténuation appropriées d'ordre technique

[56] BSK-*Niggli*/*Maeder*, art. 12 CP no. 111.

et organisationnel prises par la banque et le prestataire de service, tel que l'encryptage (en prenant en compte la gestion de la clé), et les restrictions et interdictions contractuelles imposées au prestataire de services (voir notamment para. 24 ss. du Guide).

(b) les autres risques inhérents au prestataire de services qui doivent être évalués dans le cadre du processus de sélection et d'adjudication, atténués par le biais de MTOs adéquates, et le cas échéant acceptés, ce qui comprend notamment l'implication de sous-traitants et du soutien en cas de migration (voir para. 13 ss. du Guide).

70 La banque doit également conclure des accords contractuels appropriés avec le prestataire de services, contrôler de manière appropriée le respect de ces accords et, si nécessaire, les faire respecter (voir para. 12 du Guide).

71 En cas d'externalisation à l'étranger – ou si un accès à des CID depuis l'étranger est accordé (ce qui est équivalent dans une large mesure) – les risques spécifiques à l'étranger doivent également être pris en compte, y compris notamment :

(a) le lieu où les CID sont ou peuvent être stockées durant la période d'exécution du contrat ou de traitement et à partir d'où il peut y être accédé.

(b) les risques juridiques encourus par le prestataire de services en cas de violation de la légalisation étrangère qui lui est applicable, p. ex. d'éventuelles sanctions et le risque associé que le prestataire de services à l'étranger n'agisse pas avec la même diligence qu'un prestataire de services suisses en raison d'une absence ou d'un risque moindre de responsabilité pénale. A cet égard, il serait toutefois irréaliste de supposer que la seule menace des sanctions prévues à l'art. 47 al. 1 et 2 LB puisse empêcher un prestataire de services de transmettre des CID à des tiers non autorisés. Le risque réputationnel a certainement plus de poids en ce qui concerne, en tout cas, les fournisseurs actifs dans le monde entier, lesquels auraient à craindre d'énormes dommages si un transfert non autorisé de CID était découvert. Les restrictions de droit étranger, telles que le § 203 du code pénal allemand ou la menace d'amendes en vertu du Règlement européen sur la protection des données (art. 83 RGPD) jouent également un rôle dans ce contexte, bien que dans une moindre mesure peut-être.

(c) les possibilités d'accès (en droit et en fait) des autorités locales dans les juridictions concernées et les risques qui en découlent pour le client de la banque[57], ainsi que

(d) les possibilités pour la banque et son client de se défendre par des moyens légaux contre un accès aux CID (compte tenu du fait que le risque d'accès dans le cadre d'une procédure étatique existe également dans le cas de données situées en Suisse, que l'externalisation à l'étranger n'est en soi pas interdite, et que des motifs justifiant une demande d'accès sont concevables, la banque s'acquitte généralement de ses obligations de diligence, lorsqu'elle s'assure qu'elle-même ou les clients concernés peuvent faire examiner la requête dans le cadre d'une procédure étatique).

(e) les possibilités d'accès (en droit et en fait) par des autorités extérieures aux juridictions concernées en raison d'une externalisation spécifique, par exemple dans le cadre d'une ordonnance requérant la divulgation de données stockées en dehors du territoire concerné. Tel est notamment le cas, par exemple, du US CLOUD Act, lequel prévoit la disposition suivante dans le Stored Communications Act[58] (Sec. 103(a)(1))) :

> *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.*[59]

---

[57] Le risque qu'une autorité ait accès au CID existe également en Suisse et ne viole pas, en principe, le secret bancaire. Seul le risque additionnel encouru par le client d'un accès au CID par une autorité étrangère ou les autorité étrangère compétentes doit être pris en compte dans ce contexte.

[58] Pub.L. 99-508.

[59] Dans le cas de données relatives à des personnes qui ne sont ni des citoyens américains ni résidents aux Etats-Unis, la divulgation de données peut être empêchée par une tribunal si l'état dans lequel les données sont conservées a conclu un accord avec les Etats-Unis ; voir Determann/Nebel, U.S. CLOUD Act – Nuages sur les règlements fondamentaux de protection des données? in : CR 6/2018, 408-412, 410.

(f) le risque que des autorités locales puissent accéder aux CID en violation des principes de l'état de droit, à savoir, par exemple, lorsque le risque d'accès pour des raisons purement fiscales ou politiques est plus élevé qu'un accès fondé sur un soupçon fondé d'infraction pénale.

(g) les informations disponibles, permettant une bonne évaluation de ces risques à l'étranger.

72 Les évaluations de risque, les analyses, les conclusions et les mesures entreprises doivent être documentées et actualisées, si nécessaire.

73 En cas de manquement à l'obligation de diligence, les développements effectués aux para. N 39 ss. et 65 sont applicables sous l'angle du droit pénal. En plus de l'obligation de diligence, la banque peut être tenue d'adopter d'autres mesures, ne faisant pas l'objet du présent rapport, sur la base d'autres dispositions applicable, y compris notamment en matière de secret et de protection des données.