LAUX LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
A Seegartenstrasse 2
P. O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LLM
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen
Anwaltsregistern eingetragen

Avis juridique

Utilisation de services Cloud par les banques: concernant la recevabilité selon l'art. 47 LB

En même temps une contribution à la discussion à l'occasion de la publication d'un guide sur le Cloud de l'Association Suisse des Banquiers (ASB) concernant l'utilisation des services Cloud par les banques et les négociants en valeurs mobilières

(Traduction pratique de l'original Allemand)

Auteurs:
Dr Christian Laux
Alexander Hofmann
Mark Schieweck
Dr Jürg Hess

Zurich, le 14 février 2019

MANAGEMENT SUMMARY

Objet: Le présent avis juridique examine dans quelle mesure et sous quelles conditions une banque[1] est habilitée à utiliser les services Cloud[2]. L'analyse se limite à l'aspect pénal du secret bancaire et repose sur trois questions concrètes:

- Question 1: (a) Une banque suisse est-elle habilitée à utiliser des services Cloud au sens de l'art. 47 de la loi fédérale sur les banques et les caisses d'épargne (Loi sur les banques, **LB**)? (b) La réponse est-elle différente pour les services Cloud à composante internationale[3]?
- Question 2: (a) Peut-on faire appel à un fournisseur de services Cloud[4] en tant que «mandataire» au sens de l'art. 47 LB et la migration de données bancaires de clients au fournisseur de services Cloud constitue-t-elle une impunité au sens de l'art. 47 LB? (b) La réponse est-elle différente pour les services Cloud à composante internationale?
- Question 3: L'article 47 LB autorise-t-il un fournisseur de services Cloud qui n'a pas été désigné comme mandataire à accéder à des informations protégées par le secret bancaire, pour autant qu'il le fasse uniquement à des fins opérationnelles (notamment à des fins de maintenance ou de support informatique)?

Résultat au préalable: Selon le point de vue exprimé ici, l'utilisation des solutions Cloud matures en Suisse et à l'étranger est également autorisée pour les banques. En tant qu'utilisateur, la banque doit soigneusement sélectionner le fournisseur de services Cloud et prendre les mesures appropriées pour s'assurer que les données migrées soient protégées dans la même mesure dans les infrastructures informatiques[5] du fournisseur de services Cloud. L'objectif de ces mesures vise à éviter les divulgations relevant du droit pénal dans le cours normal des opérations[6]. Pour pouvoir le garantir à long terme, la banque doit comprendre le fonctionnement du périmètre étendu par le service Cloud. Cette situation doit être sécurisée par des mesures contractuelles. Ce principe est tiré de ce qui suit:

Question 1: Si la banque choisit des fournisseurs de services Cloud capables de garantir, sur le plan technique, organisationnel et contractuel, qu'aucune divulgation ne sera possible à des tiers non autorisés dans le cours normal des opérations, la banque est habilitée à utiliser leurs services Cloud. L'expérience montre que cela peut déjà être assuré aujourd'hui par des fournisseurs de services Cloud matures. La migration des données vers les infrastructures informatiques de ces fournisseurs de services Cloud ne remplit pas l'élément constitutif de l'infraction («divulgation»). Cela signifie qu'il n'y a à priori pas de comportement punissable par la loi, quelle que soit la réponse aux questions 2 et 3 (sous-question 1a). La question de la composante internationale n'est pas pertinente pour ces services Cloud (sous-question 1b).

---

1 Voir en annexe le terme «banque».
2 Voir en annexe l'expression «services Cloud».
3 Voir en annexe le terme «composante internationale».
4 Voir en annexe le terme «fournisseur de services Cloud».
5 Voir en annexe le terme «infrastructures informatiques».
6 Voir en annexe le terme «cours normal des opérations.».

Question 2: Un fournisseur de services Cloud peut être désigné comme mandataire au sens de l'art. 47, al. 1, let. a, LB. Cela permet d'étendre le périmètre de la banque, sur le plan des ressources humaines. La banque doit s'assurer que le fournisseur de services Cloud a mis en œuvre des mesures de protection de nature technique, organisationnelle et contractuelle. La migration des données vers les infrastructures informatiques du fournisseur de services Cloud ne constitue pas une divulgation (**effet de privilège** en matière pénale, au profit des personnes agissant pour le compte de la banque). Ceci s'applique également si les employés du fournisseur de services Cloud ont la possibilité technique d'accéder aux textes en clair[7] concernant les données de la banque. Inversement, l'effet de privilège n'est pas automatique. Un fournisseur de services Cloud peut refuser l'intégration dans la sphère de risque de la banque. Si le fournisseur de services Cloud possède le niveau de maturité mentionné à la question 1, la banque peut toujours utiliser le service Cloud.

L'effet de privilège peut également être affirmé lors de la migration des données vers les infrastructures informatiques d'un fournisseur de services Cloud à composante internationale. Le facteur déterminant pour ce résultat est le libellé de la disposition de l'art. 47 al. 1 let. a LB. Il n'exclut pas le recours à des mandataires à composante internationale. L'art. 1 CP («pas de sanction sans loi») exclut un traitement différent des services Cloud à composante internationale. Ce résultat doit être étayé par une interprétation complémentaire de la disposition pénale de l'art. 47 LB. Le résultat de cette interprétation est que la responsabilité pénale ne peut pas être maintenue aujourd'hui si des mandataires à composante internationale sont mandatés.

L'effet de privilège permet à la banque d'utiliser les fournisseurs de services Cloud même si le fournisseur (ou ses employés ou sous-traitants) peut obtenir un accès contrôlé aux données soumises au secret bancaire en texte clair dans le cours normal des opérations (sous-question 2a). Cela s'applique également aux fournisseurs de services Cloud à composante internationale (sous-question 2b).

Question 3: En ce qui concerne la dernière question posée, la question 3, la marge de manœuvre est restreinte après la réponse aux questions 1 et 2. Si le fournisseur de services Cloud a été désigné comme mandataire, le problème ne se pose pas en soi (échange privilégié d'informations possible sans conséquences pénales). Pour bon nombre des mesures opérationnelles dont il sera question à la question 3 concernant les fournisseurs de services Cloud matures, on pourra confirmer qu'aucune divulgation n'a lieu (dans ce cas, l'analyse de la question 1 s'applique alors à priori). Si le support par des employés d'un fournisseur de services Cloud qui n'a pas été désigné comme mandataire conduit à un accès aux informations des clients de la banque en texte clair, la banque est tenue de mettre en place un mécanisme de contrôle justifiable (par exemple: uniquement un accès «*just in time*», c'est-à-dire, un accès seulement au cas par cas; un accès seulement s'il y a un besoin avéré «*need to know*»; dans chaque cas sous le contrôle de la banque, «*4 eyeballs principle*»; en principe sans transfert des compétences de contrôle par l'employé de support externe, «*least privilege*»). Si ce principe est mis en œuvre de manière appropriée, la responsabilité pénale de la banque peut être évitée, même sans désignation d'un mandataire.

Pour résumer: l'utilisation du Cloud par les banques peut être confirmée comme légale sur la base de l'état actuel de la technique, de la doctrine et de la juridiction. La banque peut également faire appel à des fournisseurs de services Cloud matures si ceux-ci n'acceptent pas l'intégration dans le périmètre des ressources humaines de la banque, pour autant que la solution Cloud soit suffisamment protégée contre

[7] Voir en annexe l'expression «accéder aux textes en clair».

la divulgation au moyen de mesures techniques, organisationnelles et contractuelles, conformément aux réponses aux questions 1 et 3. Quoi qu'il en soit, la banque doit veiller à la mise en œuvre de mesures techniques, organisationnelles et contractuelles et exiger une pleine transparence de la part du fournisseur de services Cloud. La banque doit tenir compte de la maturité technique et organisationnelle du fournisseur de services Cloud et comprendre comment ce dernier traite les données qu'il migre vers ses infrastructures informatiques.

PARTIE 1 NOTIONS DE BASE

I. Motif et objet

A. Motif du présent avis juridique

1 L'Association Suisse des Banquiers (**ASB**) a élaboré un guide sur l'utilisation des services Cloud par les banques et les négociants en valeurs mobilières. En ce qui concerne le secret bancaire, l'ASB pose les questions spécifiques suivantes:

a. Question 1: (a) Une banque suisse est-elle habilitée à utiliser des services Cloud au sens de l'art. 47 LB? (b) La réponse est-elle différente pour les services Cloud à composante internationale?

b. Question 2: (a) Peut-on faire appel à un fournisseur de services Cloud en tant que «mandataire» au sens de l'art. 47 LB et la migration de données bancaires de clients au fournisseur de services Cloud constitue-t-elle une impunité au sens de l'art. 47 LB? (b) La réponse est-elle différente pour les services Cloud à composante internationale?

c. Question 3: L'article 47 LB autorise-t-il un fournisseur de services Cloud qui n'a pas été désigné comme mandataire à accéder à des informations protégées par le secret bancaire, pour autant qu'il le fasse uniquement à des fins opérationnelles (notamment à des fins de maintenance ou de support informatique)?

2 LAUX LAWYERS AG souhaite participer à la discussion dans le cadre de l'ASB et, pour ce faire, alimente le débat avec le présent avis juridique. Le présent avis juridique ne constitue pas une évaluation du projet de guide sur le Cloud.

3 LAUX LAWYERS AG est un cabinet d'avocats, dont la spécialisation repose sur l'interface entre le droit et les technologies de l'information. Les avocats de LAUX LAWYERS AG possèdent de nombreuses années d'expérience dans le secteur financier (y compris en tant que conseillers juridiques internes pour de grandes banques suisses et des sous-traitants informatiques internationaux). LAUX LAWYERS AG conseille des clients du secteur financier en matière de droit informatique ainsi que des fournisseurs de services Cloud suisses et étrangers dans leurs relations avec les banques.

B. Objet

4 Le présent avis juridique examine dans quelle mesure et sous quelles conditions une banque est habilitée à utiliser les services Cloud. L'analyse se limite à l'aspect pénal du secret bancaire (art. 47 LB) et se fonde sur les trois questions de l'ASB mentionnées ci-dessus. D'autres sujets ne font pas

l'objet du présent avis juridique.[8] Les termes et expressions utilisés dans le présent avis figurent à l'annexe 1.

C. Protection du secret bancaire signifie protection du périmètre

5 Toute personne qui garde un secret pour un tiers doit s'assurer que ce secret ne soit pas divulgué à un tiers non autorisé. La personne qui garde le secret atteint cet objectif en protégeant sa sphère d'influence et de risque contre les fuites qui risquent de divulguer le secret à des tiers. Dans le présent avis juridique, nous décrivons ce devoir de protection comme un devoir de protéger son propre périmètre. Il traite entre autres de la sécurité et du contrôle d'accès. La protection du périmètre présente au moins les trois caractéristiques suivantes:

- Le **périmètre physique** doit être protégé: Les bâtiments, etc., doivent être protégés contre l'accès par des personnes non autorisées; cela s'effectue principalement par des mesures structurelles.

- Le **périmètre logique** doit être protégé: Les réseaux et autres infrastructures informatiques doivent être protégés contre l'accès logique par des tiers non autorisés (pirates informatiques, etc.).

- Le **périmètre des ressources humaines** doit être protégé: Dans une économie aussi spécialisée qui est la nôtre, plus personne ne travaille seul. Une banque, par exemple, doit néanmoins pouvoir répondre à tout moment à la question «où commence et où finit la banque». Cela s'effectue par le biais de contrats appropriés avec les personnes et entreprises qui supportent la banque dans sa tâche.

6 Du point de vue du client de la banque, ce qui précède se présente comme suit: le client de la banque conclut un contrat avec la banque en tant qu'institution et se fonde sur la confidentialité à l'égard des personnes extérieures à la banque. Au sein de la banque, il s'attend à ce que des mesures efficaces soient prises pour protéger ses données à caractère personnel.

---

8 Le présent avis juridique ne traite notamment pas des circulaires de la FINMA (Circ. 2018/3 «Outsourcing – Banques et assurances» et Circ. 2008/21 «Risques opérationnels»), des aspects relatifs à la protection des données, des restrictions qu'une banque peut s'être imposées dans le cadre de directives internes ou auxquelles elle s'est engagée dans le cadre de contrats avec des clients bancaires ou des tiers, des aspects relatifs à l'accès par les autorités (par exemple LSCPT ou d'autres sujets spéciaux tels que le CLOUD-Act, l'accès d'autorités, etc.); les dispositions du Code pénal suisse (art. 273 CP, etc.). Des explications pratiques sur la mise en œuvre (par exemple, la description complète d'une solution concrète, la discussion de mesures techniques, organisationnelles ou contractuelles individuelles ou des combinaisons de ces mesures; les informations sur la manière dont la banque planifie une migration dans le Cloud; les catalogues d'exigences qu'une banque devrait établir afin de mettre en œuvre la migration dans le Cloud de manière organisationnelle; les catalogues d'exigences afin de couvrir les exigences en matière de Compliance; les mesures d'information vis-à-vis des clients des banques) ne sont traitées que de manière marginale.

II. Informations générales sur le secret bancaire

A. Bases juridiques

1. Base contractuelle

7 Fondement contractuel: La relation entre une banque et ses clients est essentiellement de nature contractuelle. Une banque tient au moins un compte pour un client sur la base d'un accord spécifique et est soumise à l'obligation de rendre compte. Dans le cadre de ces accords, la banque assume également l'obligation de protéger les informations obtenues sur le client. Dans la plupart des cas, la banque modifie les dispositions du Code suisse des obligations (CO) résumées ci-dessous. En règle générale, la relation commerciale avec le client est décrite et réglée dans les Conditions générales de vente (**CGV**).

8 Principes complémentaires: La confidentialité serait également une obligation secondaire de la banque à l'égard du client de la banque si l'accord contractuel concret (N 7) ne traitait pas de cet aspect. En vertu de l'art. 398 al. 2 CO, les mandataires sont responsables envers le mandant de la bonne et fidèle exécution du mandat confié. Dans ce contexte, la banque est mandatée d'effectuer une transaction avec le client de la banque (le mandant). L'art. 398 al. 2 CO oblige également la banque à sauvegarder l'intégrité morale et personnelle du client de la banque. Cela inclut l'intérêt du client de la banque à la sauvegarde de ses droits de la personnalité au sens de l'art. 28 du Code civil suisse (**CC**). Les informations relatives à l'existence de la relation bancaire ainsi que d'autres informations doivent également être protégées par la banque au sens de l'art. 28 CC.

2. Renforcement de la protection contractuelle par l'art. 47 LB

9 Le secret bancaire ainsi défini bénéficie d'une protection supplémentaire en vertu de diverses dispositions de la réglementation de droit public des marchés financiers, dont la plus importante et la plus pertinente dans la pratique est l'art. 47 LB.[9]

10 En outre, le droit de la protection des données et le droit administratif renforcent également le secret bancaire (par exemple l'annexe 3 de la Circulaire 2008/21 de la FINMA). Toutefois, cette question ne sera pas abordée plus en détail ici.

3. Considérations supplémentaires

11 La description ci-dessus de la base juridique en matière de secret bancaire démontre que le secret bancaire est issu avant tout du droit privé (voir supra N 7 ss.). L'horizon d'attente du client de la banque est donc important (**intérêts relatifs à l'intégrité et à la protection de la personnalité**). Le client de la banque attend de la banque *qu*'elle protège son périmètre avec des moyens établis (voir N 5). Sous ces conditions, le client de la banque accepte le traitement de ses informations

---

9 Des dispositions pénales similaires figurent notamment dans d'autres lois relatives au marché financier suisse (art. 43 de la Loi fédérale sur les bourses et le commerce des valeurs mobilières (LBVM), art. 147 de la Loi fédérale sur les infrastructures des marchés financiers et le comportement sur le marché en matière de négociation de valeurs mobilières et de dérivés (LIMF) et art. 148 al. 1 let. k de la Loi fédérale sur les placements collectifs de capitaux, LPCC)). Ces dispositions ne sont pas examinées plus en détail dans le présent avis juridique.

financières particulièrement sensibles. Toutefois, le client de la banque n'a pas besoin de connaître la *nature des mesures* prises par la banque pour protéger son périmètre.

12 Du point de vue de la banque, l'activité bancaire est protégée par la **garantie de propriété et la liberté économique.** La banque peut décider de manière autonome quelle entreprise et quelle politique commerciale elle souhaite mener et par quel moyen (légal) elle souhaite le faire. Il s'agit notamment de décider quelles infrastructures informatiques et quelle organisation informatique la banque souhaite utiliser. Il n'appartient pas au client de la banque de décider comment la banque s'organise. Le choix des moyens est laissé à la banque et celle-ci n'a pas à apporter des informations à ce sujet *tant qu'elle reste dans le cadre de ce qui est attendu et approprié.*

13 La banque peut également compter sur le fait que le client de la banque ne s'opposera pas à son organisation interne tant que la banque maintiendra des mesures appropriées pour sécuriser son périmètre. À cet égard, le **principe de confiance** s'applique. *Dans la mesure où la banque prend des mesures de protection appropriées, elle peut donc présupposer le consentement implicite du client de la banque.*

14 En outre, les derniers développements législatifs revêtent une grande importance: le secret bancaire n'offre pas au client de la banque une protection absolue contre la divulgation de ses données à des tiers.[10] L'horizon des attentes du client de la banque n'est donc pas le seul facteur déterminant. En effet, le secret bancaire peut être levé sans le consentement du client et même contre ses intérêts, par exemple en matière fiscale.[11] L'**intérêt public dans un système financier mondial intégré** («Level Playing Field»)[12] peut l'emporter sur les intérêts de l'intégrité et de la protection de la personnalité. Cette récente pondération législative est d'une grande importance pour l'intérêt de la poursuite pénale de l'État selon l'article 47 LB.

B. Éléments objectifs

1. Remarque préliminaire

15 L'art. 47 LB sanctionne pénalement la violation du secret bancaire. Le terme «divulgation» est le concept central de la règle de pénalité, et dans le contexte du présent avis juridique, la considération doit se limiter à ce concept. Les autres éléments constitutifs de l'infraction – notamment la notion de secret – sont suffisamment décrits dans la littérature pertinente.

---

[10] FF 1970 I 1144 ss., 1161: «*Es muss hier gleich mit allem Nachdruck betont werden, dass das Bankgeheimnis nicht unbeschränkt gilt und keinen Deckmantel für Delikte darstellt. Artikel 47 des Bankengesetzes bestraft bloss die widerrechtliche Verletzung des Bankgeheimnisses.*» (*Traduction de la citation*: *«Il importe d'entrée de bien insister sur le fait que ce secret bancaire n'est pas illimité et qu'il ne saurait couvrir des délits. L'article 47 LB ne punit que les infractions aux dispositions du secret bancaire.»)*

[11] Depuis 2017, par exemple, les données bancaires sont automatiquement collectées et échangées entre les pays qui se sont engagés à appliquer la norme mondiale d'échange automatique de renseignements (EAR). Pour plus de détails, voir infra, N 47.

[12] FF 2017 4913 ss., 4935.

16 D'après la jurisprudence suisse, il n'existe pas de jurisprudence qui clarifie ou même traite de la notion de divulgation en relation avec l'informatique dans le Cloud en général ou avec les offres dans le Cloud en particulier. En conséquence, il convient d'examiner et de préciser si le transfert de données dans les infrastructures informatiques d'un fournisseur de services Cloud constitue un acte de divulgation au sens de l'art. 47 LB.

2. Concernant la notion de «divulgation» dans la doctrine et la jurisprudence

17 Le tribunal fédéral a récemment statué qu'une divulgation n'existe que lorsqu'un tiers a effectivement perçu l'information à protéger.[13] C'est ce que nous appelons ici l'accès en texte clair[14]:

> *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 (DONATSCH/THOMMEN/WOHLERS, Strafrecht IV, 5. Aufl. 2017, S. 580 f.; siehe auch NIGGLI/HAGENSTEIN, in: Basler Kommentar, Strafrecht II, 3. Aufl. 2014, N. 36 zu Art. 162 StGB). 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. Der angefochtene Entscheid ist bereits aus diesem Grund aufzuheben.*
>
> *(Traduction de la citation: «Dans l'arrêt du TF 142 IV 65 E. 5.1 mentionnée par l'instance précédente, le Tribunal fédéral a considéré qu'un secret est considéré divulgué que s'il est porté à la connaissance d'un tiers non autorisé ou si l'on permet à ce tiers de l'obtenir. Il s'agit simplement d'une description du comportement punissable dont – contrairement à l'opinion de l'instance précédente – rien ne peut être déduit au moment où l'infraction a été commise. Dans cette question, il faut plutôt suivre la doctrine selon laquelle l'infraction est commise dès qu'un tiers prend connaissance du secret en question en raison du comportement de l'auteur de l'infraction. Une tentative punissable pourrait être notamment présumée, si l'auteur de l'infraction a rendu les informations accessibles à un tiers, mais celui-ci n'a pas encore pris connaissance du secret (DONATSCH/THOMMEN/Wohlers, Droit pénal IV, 5. Édition. 2017, p. 580 ss.; voir aussi NIGGLI/HAGENSTEIN, dans: Commentaire de Bâle, Droit pénal II, 3e édition 2014, n. 36 à l'art. 162 CP). Aucun des employés de B._____ Sagl n'a pris connaissance des dessins trouvés dans les papiers destinés au recyclage. Une condamnation pour violation du secret de fabrication ou de fabrique est donc exclue dès le départ. La décision contestée doit déjà être annulée pour ce motif.*

18 La violation du secret bancaire peut donc être qualifiée de **délit matériel.** La divulgation signifie donc «rendre disponible» les informations, c'est-à-dire les informations qui ont en soi un sens[15] *et* qui peuvent être consultées concrètement.[16] S'il n'y a pas d'accès en texte clair, les éléments constitutifs de l'infraction objectifs de l'art. 47 LB ne sont pas non plus remplis. S'il n'y a pas d'accès en texte clair, le motif n'est pas pertinent (si l'accès est absolument impossible ou s'il n'a manifestement pas eu lieu). Par exemple, aucune divulgation n'a lieu si une personne non autorisée a le

---

13 TF 6B_1403/2017 du 8 août 2018, E. 1.2.2; RSJ114/2018 p. 453.

14 Pour le terme «accès en texte clair», voir aussi la définition dans l'annexe.

15 Les informations non «parlantes». qui sont cryptées, rendues anonymes ou nécessitent un dispositif technique pour être lues.

16 Exemple: Si le détenteur du secret tient une feuille de papier portant un secret devant une personne non autorisée à une distance de 5 m, aucune divulgation n'a lieu si la personne non autorisée ne peut lire le texte à cette distance; toutefois, si la personne non autorisée a un téléobjectif devant elle à travers lequel elle peut lire le texte, une divulgation a lieu.

contrôle physique temporaire d'un support, mais n'a aucun moyen de lire les informations stockées sur ce support.

19 La qualification de délit matériel ne correspond pas à la doctrine prédominante[17] et à la juridiction[18], mais elle est néanmoins correcte. Il faut, comme l'affirme le Tribunal fédéral, distinguer les *comportements* ou les *actes* qui provoquent ou peuvent provoquer une divulgation de leur effet (c'est-à-dire la *survenance du résultat* ou la *divulgation* en tant que telle [19]). Le monde moderne rend cette distinction nécessaire.[20]

20 En outre, une différenciation supplémentaire doit être faite au niveau de l'*acte* qui entraîne une divulgation. Dans le passé, la doctrine et la juridiction se concentraient toujours sur la *perpétration active* de l'acte, par exemple à travers ce qui suit:

- **L'auteur fournit à un tiers non autorisé un accès direct en texte clair aux informations protégées.** Exemple: Communication à un expert des faits d'un litige.[21] Dans la mesure où

---

17 En lieu et place de nombreuses publications: Damian K. Graf, Sur les limites d'application du Droit pénal suisse lors de violations de secrets d'affaires, RSJ 112 (2016) 19 ss., 197: «*Zunächst ist festzuhalten, dass es sich bei den Geheimnisverratsdelikten um schlichte Tätigkeitsdelikte handelt, ...» "(Traduction de la citation: «Il convient tout d'abord de noter que les délits de violation de secrets sont des purs délits d'action,...»)*, a.d.i.s..; Andreas Donatsch, Droit pénal III, Delikte gegen den Einzelnen (Délits contre l'individu), 10e édition, Zurich 2013, p. 336; Olivier Weniger, La protection des secrets économiques et du savoir-faire [Know-how], Diss. Lausanne, Genève 1994, p. 256; Georges Bindschedler, Der strafrechtliche Schutz wirtschaftlicher Geheimnisse (La protection pénale des secrets économiques), Diss. Berne, Berne 1981, 57 ss et 72; pour la qualification de délit matériel dans le cadre du secret professionnel de l'avocat: Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (Expertise sur l'utilisation des services Cloud par les avocats pour le compte de la Fédération suisse des avocats (FSA)), p. 13 ss.

18 TPF SK.2017.52 du 4 avril 2018, E. 4.2.2: «Umstritten ist, ob die Tat erst mit der Kenntnisnahme durch den Geheimnisempfänger oder bereits mit der Übergabe oder der Einräumung der Möglichkeit der Kenntnisnahme des Geheimnisses an Dritte vollendet wird (vgl. auch Urteil des Bundesstrafgerichts SK. 2016.14 vom 16. Mai 2017 E. 2.2.2). Das Bundesgericht hat sich dazu bislang, soweit ersichtlich, nicht direkt geäussert.» (Traduction de la citation: «Il est controversé si l'acte n'est accompli que lorsque le destinataire du secret en prend connaissance ou déjà lorsque le secret est remis ou qu'il a la possibilité de le faire connaître à des tiers (voir également l'arrêt du Tribunal pénal fédéral SK. 2016.14 du 16 mai 2017 E. 2.2.2). Jusqu'à présent, le Tribunal fédéral ne s'est pas exprimé, jusqu'à ce jour, directement sur cette question.»)

19 Du moins, pas clairement: Giuseppe Muschietti, Wirtschaftlicher Nachrichtendienst – eine richterliche Perspektive, EIZ - Europa Institut Zürich (Service de renseignements économiques – une perspective judiciaire, «Europa Institut» de l'Université de Zurich), volume/no 157, Zurich 2015, 113 ss., 135 ss.: «*Die Straftat ist vollendet, sobald der Destinatär in der Lage ist, das Geheimnis - auch nur teilweise - zur Kenntnis zu nehmen.*» *(Traduction de la citation: «Le délit est accompli dès que le destinataire est en mesure de prendre connaissance du secret, même partiellement.»)*

20 À ce propos, voir MARC AMSTUTZ sous: https://www.rechtimkontext.de/en/events/event/rechte-an-daten (visité le 14.02.2019): «*Und was sind eigentlich Daten? Die meisten JuristInnen begreifen Daten von ihrem Inhalt (content) her, d.h. als Information. Sie denken semiotisch. Nur: die Digitalität kennt keine Semiotik. Sinnieren sie über Digitalität, tun sie das in den Kategorien der Hermeneutik. So wurden sie ausgebildet. Nur: die Digitalität kennt keine Hermeneutik. Verpassen sie die Idiosynkrasien der Digitalität? Lavieren bringt hier nichts: JA, vollends. Nicht einmal die Schlüsselfrage der Digitalität vermögen sie heuristisch zu fassen. Kein Wunder.» (Traduction de la citation: «Qu'entend-on sous données? La plupart des avocats comprennent les données à partir de leur contenu (content), c'est-à-dire comme des informations. Ils pensent sémiotiquement. Seulement: le numérique ne connaît pas la sémiotique. S'ils pensent à la numérisation, ils le font dans les catégories de l'herméneutique. C'est ainsi qu'ils ont été formés. Seulement: le numérique ne connaît pas l'herméneutique. Ne comprennent-ils pas les particularités de la numérisation? Pas la peine de tergiverser: OUI, complètement. Ils ne sont même pas capables de saisir la question clé de la numérisation heuristiquement. Ce n'est guère étonnant.»* Marc Amstutz écrit ceci en guise d'introduction à une présentation dans le cadre de sa recherche sur la propriété de l'information (Marc Amstutz, Dateneigentum – Funktion und Form (Propriété des données – fonction et forme), AcP 218 [2018], 438 ss.). Marc Amstutz aborde également la même divergence dans un article intitulé «Dateneigentum – Eckstein der kommenden Digitalordnung» (Propriété des données – pierre angulaire de l'ordre numérique à venir) dans la Neue Zürcher Zeitung, septembre 2018, 10e édition.

21 TC ZH UE140317 du 9 juillet 2015: «*Offenlegung von allfälligen Bankgeheimnissen gegenüber einem externen Privatgutachter [kann] tatbestandsmässig sein (...)». (Traduction de la citation: «La divulgation de secrets bancaires éventuels à un expert privé externe [peut] réunir tous les éléments constitutifs de l'infraction (...)».*

une procédure technique est encore nécessaire pour la lecture ou le contrôle, la simple accessibilité des données pour les «tiers» ne constitue pas en soi un accès en texte clair au titre du présent tiret.[22]

- **Créer une situation où des tiers peuvent avoir accès en texte clair à l'information protégée.**[23] Exemple: Envoi d'un CD-ROM à un destinataire qui peut lire le contenu du CD.[24] Dans ce scénario, le fait qu'une personne non autorisée ait accès à des données contenant les informations protégées peut déjà être sanctionné[25] (de l'avis exprimé ici, cependant, seulement si le tiers «ouvre» les données et lit le contenu par la suite (voir ci-après).

21 Le Tribunal fédéral admet également que dans la deuxième variante, la sanction pour tentative est toujours possible (l'auteur est puni selon sa conception, issue de l'élément constitutif de l'infraction subjectif). La condition en est la connaissance et à la volonté de l'auteur de l'infraction en ce qui concerne la divulgation (art. 22, al. 1 CP; une tentative commise par négligence est inconcevable). Bien que de tels scénarios soient concevables, ils ne font pas l'objet du présent avis juridique. Il convient plutôt de clarifier si une banque peut se positionner de sorte qu'elle *ne se rende justement pas pénalement punissable* lorsqu'elle utilise des services Cloud. Plus précisément: qu'est-ce que la banque ne devrait pas ignorer pour éviter une responsabilité pénale? Dans ce qui suit, nous traiterons donc exclusivement de l'art. 47 LB comme un *délit d'omission improprement dit, sous la forme d'une infraction commise par négligence.*

3. Délit d'omission

22 La banque en tant que garante: L'art. 47 al. 1 LB est structuré à la fois par les éléments constitutifs de l'infraction de base (délit intentionnel) et dans l'al. 3 (délit par négligence) (art. 10 al. 3 du Code pénal) qui punit aussi toute personne restant inactive alors qu'elle a une obligation d'agir (art. 11 al. 1 du Code pénal). Dans le cadre de la relation d'affaires, le client de la banque confie à la banque des informations sur sa situation personnelle et s'attend à ce que la banque prenne les mesures appropriées pour protéger ces informations (N 11). L'obligation de prendre des mesures de protection découle du contrat. À cet égard, la banque est la *garante* de la protection de l'intégrité morale et personnelle (N 8) du client de la banque.

23 Obligations de protection: Si la banque enregistre des données dans des infrastructures informatiques tierces, cela ne constitue pas automatiquement une violation de contrat. La banque doit garantir une protection de périmètre suffisante (voir supra N5). Cela signifie que la banque doit prendre des **mesures de protection suffisantes** pour empêcher les personnes non autorisées de prendre connaissance du contenu du secret, c'est-à-dire d'accéder à un texte clair dans le cours

---

22 Toutefois, un tel événement doit être examiné dans le cadre du deuxième aspect de la règle («Créer une situation dans laquelle les tiers sont en mesure d'obtenir des informations sur des informations confidentielles»).

23 Wolfgang Wohlers, Auslagerung einer Datenbearbeitung und Berufsgeheimnis (Externalisation du traitement des données et du secret professionnel) (Art. 321 CP), digma Schriften zum Datenrecht (Ouvrages sur les droits en matière de données), volume 9, Zurich 2016, p. 17 a.d.i.s.

24 TC ZH SB110200 du 19 août 2016: «*Durch den Versand der CD an die Steuerbehörden und die Zeitschrift "Cash" hat der Beschuldigte dieses Geheimnis offenbart.» (Traduction de la citation: «En envoyant le CD à l'administration fiscale et au magazine «Cash», la défenderesse a divulgué ce secret.»)*

25 Au regard de l'art. 321 CP: TD Uster du 20 mars 1996 (ZR 96/1997, 289, 294); STEFAN TRECHSEL, Schweizerisches Strafgesetzbuch, Kurzkommentar (Code pénal suisse, bref commentaire), Zurich 1997, CP 320 N 8.

normal des opérations. Si la banque prend de telles mesures, elle se comporte conformément aux attentes du client de la banque (N 5, N 11). Si elle ne le fait pas, elle manque à ses obligations.

24 Pouvoir d'agir: La banque a le pouvoir d'appliquer ces mesures de sécurité ou, en l'absence de telles mesures, de s'abstenir d'utiliser la solution Cloud (*pouvoir d'agir*). La banque peut exiger du fournisseur de services Cloud de lui expliquer comment celui-ci protège les données qu'elle migre vers ses infrastructures informatiques. La documentation doit couvrir l'ensemble du service Cloud et décrire de manière suffisamment détaillée comment le fournisseur de services Cloud travaille pour protéger les données migrées par la banque et s'assurer qu'aucune divulgation ne soit possible. La documentation doit permettre à la banque de déterminer si les données migrées vers les infrastructures informatiques tierces continuent d'être protégées de manière adéquate. La documentation doit servir cet objectif central. La banque n'est pas obligée d'établir elle-même cette documentation; cela incombe au fournisseur de services Cloud. En d'autres termes, avant de migrer les données vers l'infrastructure informatique du fournisseur de services Cloud, c'est de la responsabilité de la banque de déterminer comment les données transférées seront ensuite protégées. Elle doit donc identifier à l'avance et, si nécessaire, éviter les risques excessifs pour l'intégrité morale et personnelle de ses clients. Elle a donc un pouvoir d'agir relevant du droit pénal.

25 Causalité hypothétique: Les possibilités techniques de l'industrie du Cloud sont aujourd'hui bien avancées. Ce à quoi peut ressembler une telle protection est décrit dans la partie 2 (partie 2, N 65 ss.). Même si de telles mesures de protection pour des raisons techniques laissent une possibilité théorique que des tiers puissent accéder sans autorisation aux données migrées vers les infrastructures informatiques du fournisseur de services Cloud en texte clair, cela ne signifie pas que de tels accès ont lieu dans le cours normal des opérations. Selon le service Cloud sélectionné, il peut même être démontré que l'accès en texte clair à des informations secrètes est totalement exclu dans le cours normal des opérations. En d'autres termes, en sélectionnant soigneusement les services Cloud à utiliser, la banque peut contrôler quelles données elle protège et comment. Si elle ne prend pas les mesures dont elle dispose et qu'une divulgation interdite se produit, la question se pose de savoir si la divulgation aurait pu être évitée par une clarification minutieuse avec le fournisseur de services Cloud. Si la réponse est affirmative, cette omission est hypothétiquement causale pour la divulgation au sens du Droit pénal. Toutefois, la banque n'est pas tenue d'assumer la responsabilité d'événements qu'elle ne peut prévoir avec suffisamment de certitude. En conséquence, la banque ne peut être tenue responsable de l'accès illégal de tiers au service Cloud si elle s'est protégée contre un tel accès par des mesures de haut niveau. Une éventuelle faillite du fournisseur de services Cloud au sens de l'art. 47 LB n'est pas non plus préjudiciable si, au cours d'une procédure de faillite, certaines divulgations surviennent et ne peuvent être évitées. De même, l'accès d'une autorité particulière ne relève pas de la sphère d'influence de la banque. Ces exemples montrent que la banque ne doit se porter garante que de ce à quoi elle devait s'attendre d'après le déroulement normal des événements, c'est-à-dire au cours normal des opérations du fournisseur de services Cloud.

26 Exigibilité: Les mesures à prendre par la banque pour protéger le périmètre doivent être *raisonnables* pour la banque. Il n'y a guère de discussion dans la doctrine quant au niveau et à la qualité des mesures à prendre pour qu'elles soient acceptées comme une protection suffisante contre l'accès de tiers à des informations secrètes. Il serait déraisonnable de s'attendre à ce que la banque garantisse que l'accès à un texte en clair soit absolument impossible. L'art. 47 LB n'est donc pas

violé car, d'un point de vue purement technique, il existe toujours une possibilité théorique qu'une personne autre que la banque puisse accéder au secret – pour autant que des mesures soient en place pour empêcher normalement les tiers non autorisés d'accéder aux informations en texte clair devant rester secrètes. La banque n'aurait pas non plus une telle obligation en ce qui concerne les données stockées sur ses propres infrastructures informatiques. Les mesures prises doivent uniquement, mais systématiquement, correspondre à *l'état actuel de la technique*[26]. Dans la mesure où la banque ne met pas tout en œuvre pour prendre de telles mesures, elle s'expose, ainsi que ses organes ou les collaborateurs déterminants, à un risque pénal.

27 Conclusion: *Les déclarations ci-dessus signifient qu'une banque (c'est-à-dire les personnes agissant en son nom) qui fournit une protection technique et organisationnelle suffisante contre un accès non autorisé ne peut pas faire l'objet de poursuites judiciaires en vertu de l'art. 47 LB.* Une banque est autorisée à utiliser de tels services Cloud conformément à l'art. 47 LB. Si, en revanche, la banque ne prend pas les mesures de protection appropriées et qu'il en résulte un succès (un accès à un texte clair, c'est-à-dire une divulgation), les employés déterminants peuvent faire l'objet de poursuites judiciaires – le droit de désigner le fournisseur de services Cloud comme mandataire au sens de l'art. 47 al. 1 LB, qui, avec le consentement des deux parties, constituant à tout moment une possibilité de conception (voir partie 1, chiffre III, N 31), reste réservé.

C. Éléments constitutifs de l'infraction subjectifs

28 Le secret bancaire peut être violé intentionnellement ou par négligence. Il n'y a pas infraction commise intentionnellement ou par négligence lorsque les organes de la banque parviennent à la conclusion que l'infrastructure informatique technique choisie par eux protège efficacement contre la divulgation à des tiers non autorisés.

29 Aucune infrastructure informatique n'offre une protection complète contre les accès non autorisés. Si les organes et employés d'une banque savent qu'il existe des risques résiduels mineurs de divulgation non autorisée, ils ne sont pas coupables d'un manquement au devoir de diligence, pourvu qu'ils aient pris des mesures de protection vis-à-vis du fournisseur de services Cloud.

30 Les personnes agissant pour le compte de la banque ne pourront être poursuivies en justice par négligence que si elles n'exercent pas la diligence due par la banque en violation de leurs obligations. Ici aussi, les mesures techniques et organisationnelles prises par la banque pour protéger ou faire protéger les informations à garder secrètes à l'égard de tiers sont déterminantes. Les organes d'une banque qui ne prennent pas de mesures de protection se comportent en violation de leurs obligations si la banque n'a pas usé des précautions commandées par les circonstances et par la situation de ses ressources humaines (art. 12 al. 3 CP). La banque doit s'assurer des mesures de sécurité appliquées au moyen d'une documentation significative et doit prévoir des contrôles efficaces.

---

26 Pour cette catégorie (personnel ou sous-traitants), la composante internationale existe si l'accès au service Cloud peut être obtenu depuis l'étranger.

III. Concernant la fonction du «mandataire» au sens de l'art. 47 al. 1 LB

A. Remarques préliminaires

31 Art. 47 LB est une véritable infraction spéciale, c'est-à-dire que les auteurs ne sont que les groupes de personnes explicitement et exhaustivement énumérés, imputables à la sphère de risque de la banque (par ex. les organes et les employés). Depuis 1971, l'art. 47 LB mentionne également expressément les mandataires, afin de permettre aux banques d'externaliser des services dans un cadre raisonnable de son domaine d'activité.[27] Il ressort clairement de ces documents que le changement intervenu à l'époque visait à rendre les prestataires de services de centres informatiques, en particulier pour les banques, passibles de poursuites judiciaires.[28] Étant donné que les mandataires font également partie du groupe des personnes punissables, la «divulgation par la banque des relations avec les clients aux mandataires»[29] est considérée comme autorisée.[30] Si le mandataire est une personne morale, les personnes agissant au nom du mandataire peuvent être considérées, en droit, conformément à l'art. 47 al. 1 let. c LB.

32 Les fournisseurs de services Cloud utilisent également des infrastructures informatiques telles que les centres de données pour leurs services et peuvent facilement être considérés comme des mandataires. L'interprétation suivante déterminera si les fournisseurs de services Cloud peuvent être des «mandataires» au sens de l'art. 47 al. 1 let. a LB.

---

[27] BSK BG STRATENWERTH, art. 47 N 7: «*Das wird man dahin verallgemeinern dürfen, dass die Bank Dritte jedenfalls dann in den Kreis der Geheimnisträger einbeziehen darf, wenn dies einem ernstzunehmenden Interesse an der Optimierung ihrer Leistungen oder an der Senkung ihrer Kosten entspricht.*» (Traduction de la citation: «*On pourra même le généraliser de manière à ce que la banque puisse en tout état de cause inclure des tiers dans le cercle des détenteurs de secrets si cela correspond à un intérêt fondé d'optimiser ses services ou de réduire ses coûts. La divulgation de données à caractère personnel dans un tel cadre devrait, en règle générale, être également dans l'intérêt bien compris du client de la banque, dont la protection est en jeu.*»

[28] FF 1970 I 1144 ss., 1182: «*Mit der Unterstellung des Beauftragten sollen insbesondere auch Rechenzentren erfasst werden, die von Banken mit der elektronischen Datenverarbeitung betraut werden.*» (Traduction de la citation: «*Notamment la subordination du mandataire devrait également inclure les centres informatiques chargés par les banques du traitement électronique des données.*»

[29] BEAT KLEINER/RENATE SCHWOB/CHRISTOPH WINZELER, dans: Zobl/Schwob/Geiger/Winzeler/Kaufmann/Weber/Kramer (éditeur), Kommentar zum Bundesgesetz über die Banken und Sparkassen (Commentaire de la Loi fédérale sur les banques et les caisses d'épargne), 23e édition, Zurich etc. 2015, art. 47 N 369: «*Die Preisgabe von Kundenbeziehungen an Beauftragte ist somit i.S.v. Art. 32 StGB grundsätzlich erlaubt. Die Erläuterung in der Botschaft ("insbesondere") lässt erkennen, dass der Wortlaut von Art. 47 Abs. 1 BankG insoweit für Entwicklungen der Zukunft nicht nur offen gehalten, sondern auch mit Absicht so formuliert wurde.*» (Traduction de la citation: «*La divulgation des relations avec les clients à des mandataires au sens où l'entend l'art. 32 CP est en principe autorisé. L'explication dans le message («notamment») montre que le libellé de l'art. 47 al. 1 LB n'a pas seulement été maintenu vague par rapport aux développements futurs, mais a aussi été délibérément formulé de cette manière.*»)

[30] BEAT KLEINER/RENATE SCHWOB, dans: Bodmer/Kleiner/Lutz (éditeur), Kommentar zum schweizerischen Bankengesetz, (Commentaire sur la Loi sur les banques), Zurich 1996, BankG 47 N 102; Urs Zulauf, Bankgeheimnis und historische Forschung,(Secret bancaire et recherche historique), ZSR 113 I (1994), 115; Peter Honegger / Thomas A. Frick, Das Bankgeheimnis im Konzern und bei Übernahmen (Le secret bancaire au sein du Groupe et dans le cadre de prises de contrôle), SZW 1996 6.

B. Fournisseurs de services Cloud en tant que mandataires en général

1. Interprétation en fonction du libellé et de l'historique législatif

33 Le législateur a volontairement maintenu vague le terme «mandataire». En particulier, l'interprétation historique montre que les termes «mandat» ou «mandataire» ne contiennent pas d'évaluation législative particulière, d'autant plus que les fournisseurs de services de centres de données purs devraient également être explicitement inclus (voir supra, N 31). Le législateur a voulu permettre que de tiers externes puissent être attribués à la sphère de risque de la banque dans un monde où la division du travail s'accroît, même si cette position n'était pas nécessairement reconnaissable d'avance pour le client de la banque. La proximité d'un fournisseur de services Cloud par rapport à un fournisseur de services de centre de données est évidente, car un fournisseur de services Cloud offre des infrastructures informatiques pour l'utilisation. La formulation et l'historique sont clairs: selon l'interprétation, les fournisseurs de services Cloud peuvent être précisément regroupés sous le terme «mandataire». Le résultat de cette interprétation est toujours d'actualité et n'a pas besoin d'être corrigé.

2. Interprétation systématique

34 Conformément à l'art. 47 LB, la loi prévoit la divulgation d'informations qui doivent être tenues secrètes (voir supra, N 17 ss.). Il est évident que de nombreuses personnes travaillant au sein de la banque ont accès aux données relatives aux clients dans des cas individuels et peuvent, dans ce cadre, percevoir le contenu sémantique stocké de ce que les données expriment (accès en texte clair). L'obligation de secret s'applique à toute personne travaillant au sein ou pour le compte d'une banque.[31] D'autres normes pénales pour la protection des secrets en droit suisse ayant la même portée s'appliquent au terme «personnel auxiliaire». Même si la LB choisit d'autres termes («employé» et «mandataire»), l'essentiel est de soumettre le personnel auxiliaire employé habituellement par la banque à la responsabilité pénale. De même que la définition de personnel auxiliaire dans la loi suisse sur le secret professionnel (art. 321 CP), la définition des personnes punissables dans l'art. 47 LB est également basée sur une compréhension fonctionnelle. Devait être punissable quiconque travaille dans ou avec une banque dans le cadre de ce qui est habituel aujourd'hui, de ce qui est socialement accepté et à ce que le client de la banque peut s'attendre (N 11) et, qui, dans ce cadre, coopère aux activités bancaires de manière qu'il puisse en principe obtenir connaissance des secrets protégés.

35 Sur cette base, la banque peut transférer une activité relative aux données secrètes à ceux qui sont passibles de la même peine (voir supra, N 31). Les droits à la protection des secrets, qui connaissent la notion de personnel auxiliaire ou de mandataire, sont fondamentalement conçus pour permettre une division du travail économiquement raisonnable. Les formes de division du travail justifiées par des faits correspondent à l'objectif[32] du droit suisse de régler les éléments

---

31 KLEINER/SCHWOB/WINZELER (note en bas de page 29) art. 47 N 360.

32 Le secret de fonction, qui manquait auparavant d'une clause relative au personnel auxiliaire, doit également être complété par une clause relative au personnel auxiliaire dans le cadre des travaux législatifs sur la loi relative à la protection de l'information, voir FF 2017 2953 ss., 3077 s.

constitutifs de l'infraction en matière de secret ainsi qu'à d'autres règles du droit suisse (art. 101 CO, art. 398 al. 3 et art. 399 al. 1 CO).

3. Interprétation téléologique

36 L'interprétation téléologique ne va pas au-delà de l'interprétation historique: Le législateur a voulu permettre aux banques de faire appel à des prestataires externes pour satisfaire leurs besoins informatiques dans des cas dûment justifiés. Les fournisseurs de services Cloud peuvent être désignés aussi comme mandataires en ce qui concerne l'élément téléologique.

4. Autres considérations sur l'interprétation: le concept de personnel auxiliaire fonctionnel et le lien avec le consentement implicite du client de la banque

37 Quiconque supporte directement la banque dans son domaine d'activité réglementé est, d'un *point de vue fonctionnel*, sur un pied d'égalité avec elle. Si cette égalité est possible, le responsable du secret ne *divulgue* pas un secret dans la banque s'il partage l'information secrète avec un autre employé, un organe ou un mandataire. D'un point de vue fonctionnel, toutes les personnes désignées dans les éléments constitutifs de l'infraction punissables par la loi deviennent membres de la même sphère de risque[33] (à savoir celle de la banque, à laquelle elles appartiennent ou pour laquelle elles fournissent des services en tant que mandataires). Dans cette sphère de risque, toute personne qui collabore au sein d'une division du travail doit pouvoir faire confiance à ses collègues.[34] Cette coexistence des principaux détenteurs de secrets n'est pas seulement nécessaire dans une économie fondée sur la division du travail, mais elle est aussi socialement acceptée (voir N 5 s. et N 13).

38 Dans la mesure où une telle coexistence de personnes détenant des informations confidentielles correspond à ce qui est attendu, on peut également supposer que le client de la banque y a donné son consentement implicite (N 13).[35] Le consentement implicite du client de la banque peut avoir été donné tacitement ou être présumé et accepté par la banque comme manifeste. D'une manière ou d'une autre, la portée du consentement est mesurée par rapport aux attentes du client de la banque. Ce consentement couvre les comportements auxquels le client de la banque pouvait et devait s'attendre.

5. Conclusion: Les fournisseurs de services Cloud peuvent être désignés comme mandataires au sens de l'art. 47, al. 1, let. a LB

39 L'interprétation à l'aide de différentes méthodes d'interprétation conduit au résultat que les fournisseurs de services Cloud peuvent être désignés comme «mandataires» au sens de l'art. 47 al. 1 let. a LB. Cela signifie que la banque peut également échanger des informations confidentielles en

---

33 Le périmètre des ressources humaines est ainsi étendu au mandataire (voir N 5).
Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller, Gutachten zur Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte im Auftrag des schweizerischen Anwaltsverbands (Expertise sur l'utilisation des services Cloud par les avocats pour le compte de la Fédération suisse des avocats (FSA)), 1er novembre 2018, p. 21.

35 Pour le droit des brevets expressément: TD ZH GG150233 du 18 novembre 2015, E. II.2.5.3.

texte clair avec un fournisseur de services Cloud, si elle le désigne correctement comme mandataire. Ce résultat peut être décrit comme privilégiant l'échange d'informations entre la banque et le fournisseur de services Cloud.

C. Désignation de mandataires à composante internationale

1. Introduction avec la problématique

40 La doctrine dominante jusqu'à présent[36] est de l'avis que l'effet privilégié (voir N.39) ne s'applique pas à un fournisseur de services Cloud à composante internationale.[37] Ce cas sera clarifié dans ce qui suit.

41 La discussion doit être menée en tenant compte du fait que les personnes mandatées, qui procèdent à une divulgation pertinente contrairement aux instructions de la banque, devraient être poursuivies à l'étranger. Selon la jurisprudence la plus récente du Tribunal fédéral, l'art. 47 LB doit être qualifié de délit matériel. Néanmoins, il n'y a guère de consensus dans la doctrine quant à savoir si le délit commis à l'étranger est punissable en chaque cas selon le droit suisse. L'art. 8 al. 1 CP fait foi.[38] Quoi qu'il en soit: si l'auteur du délit agissant à l'étranger n'entre pas volontairement en Suisse ou si l'extradition par l'État étranger échoue, des poursuites pénales à l'étranger devront en plus être engagées. Toutefois, la divulgation peut ne pas y être punissable ou l'auteur du délit peut s'attendre à ne pas être puni à l'étranger en raison des circonstances particulières qui y prévalent.[39] Il ressort déjà de ces remarques sommaires que la protection pénale des secrets de clients de la banque divulgués à ces personnes peut donc être réduite, voire totalement inexistante, dans certaines circonstances.

---

36 KLEINER/SCHWOB/WINZELER (supra 29), LB 47 N 371: «*Da im Ausland domizilierte Beauftragte trotz theoretischer Strafbarkeit dem Arm der schweizerischen Strafbehörden praktisch entzogen sind ("Over the border means out of control"), darf die Bank Aufträge, die zur Preisgabe von Kundenbeziehungen führen, nur dann ins Ausland erteilen, wenn dafür gewichtige Gründe sprechen wie z.B. beim Anschluss an ein internationales Zahlungssystem.*» *(Traduction de la citation: «Étant donné que les mandataires domiciliés à l'étranger sont pratiquement hors de portée des autorités pénales suisses («Over the border means out of control») malgré une responsabilité pénale théorique, la banque ne peut passer des ordres à l'étranger qui conduisent à la divulgation de relations clients que s'il existe des motifs sérieux de le faire, comme par exemple une connexion à un système international de paiement.»)* Même opinion: DAVID SCHWANINGER / STEPHANIE S. LATTMANN, Cloud Computing: Ausgewählte rechtliche Probleme in der Wolke (Problèmes juridiques sélectionnés dans le Cloud), dans: Jusletter 11 mars 2013, N 31; Ursula Widmer, Kurzgutachten für die Schweizerische Informatikkonferenz SIK betreffend die Nutzung von Cloud Services mit Rechtswahl von irischem Recht und Gerichtsstand Dublin durch die schweizerische öffentliche Verwaltung, (Bref avis d'expert pour la Conférence suisse d'informatique SIK concernant l'utilisation des services Cloud par l'administration publique suisse avec choix du droit irlandais et du for juridique Dublin), 2012, 7e édition.

37 En outre: Schwarzenegger/Thouvenin/Stiller, (note en bas de page 34) p. 21, note en bas de page 50, en référence su TD ZH GG150233 du 18 novembre 2015, E. II.2.5.3. pour le secret médical selon l'article 321 CP: Un secrétariat externe mandaté par un petit cabinet médical sans secrétariat serait considéré comme personnel auxiliaire, ***nonobstant le fait que le secrétariat n'effectue pas son travail en Suisse, mais en Allemagne.***

38 Voir en détail sur le droit d'application pénale dans les actes de divulgation numérique Damian K. Graf, Strafbewehrter Geheimnisverrat im grenzüberschreitenden Kontext (La criminalisation de la trahison de secrets dans un contexte transfrontalier), RSJ 112/2016, 193; Schwarzenegger/Thouvenin/Stiller, (note en bas de page 34) p. 35 s.;

39 Voir par exemple Graf (note en bas de page 17) 19 ss.: «Compte tenu de la protection peu fréquente des informations des clients de banques à l'étranger, l'exigence de réciprocité exclut régulièrement les poursuites et les condamnations pour violation de l'art. 47 LB»; voir: Jörg Schwarz, dans: Jürg-Beat Ackermann/Günter Heine, Droit pénal économique suisse, 2013, §19 N 112.

42 Ce qui suit traite donc de l'évaluation juridique de la question de savoir si l'on peut toujours considérer que la banque exerce un contrôle suffisant sur le fournisseur de services Cloud malgré la protection réduite ou inexistante en vertu du droit pénal. Si un contrôle suffisant est affirmé, l'effet privilégié (voir N. 39) ne devrait logiquement pas cesser de s'appliquer.

43 En effet, cette argumentation aurait été possible depuis 1971. Pourtant, pour autant que l'on sache, aucune banque n'a encore, en pratique, tenté de migrer sur cette base des données relatives au secret bancaire vers un centre informatique en Inde par exemple. Faut-il donc s'interroger sur le libellé de l'art. 47 LB, qui est resté inchangé depuis 1971, et sur sa réception au cours des 50 dernières années? La réponse est oui. Bien que la disposition légale n'ait pas changé, l'environnement l'a fait.

2. Interprétation de l'art. 47 al. 1 lit. a LB

a) Interprétation selon le libellé

44 Le libellé de l'art. 47 LB ne fait pas de distinction entre les employés, organes ou mandataires nationaux ou étrangers, etc. d'une banque. Selon l'interprétation grammaticale, le mandataire étranger doit être traité de la même manière que le mandataire suisse.[40] Tout autre résultat violerait l'art. 1 CP («nulla poena sine lege»).

b) Interprétation en fonction du contexte législatif

45 Lorsque la figure du mandataire a été introduite à l'art. 47 LB en 1971, la question de la composante étrangère en relation avec les mandataires (ou les services des centres informatiques) n'a pas été particulièrement discutée. Dans le cadre de la loi de 1934, l'objectif déclaré de la loi sur le secret bancaire était de protéger les données contre l'accès d'autres États. Dans son message concernant la révision de la loi sur les banques (1970), le Conseil fédéral a précisé les points suivants dans les grandes lignes de cette disposition[41]:

> *1934 hat der schweizerische Gesetzgeber es für notwendig gehalten, die privatrechtliche Pflicht des Bankiers zur Verschwiegenheit durch eine Strafandrohung in Artikel 47 des Bankengesetzes zu verstärken. Bei den Beratungen über diese Bestimmung wurde erwähnt, dass sie sich nicht nur gegen die eigentlichen Verletzer des Bankgeheimnisses, sondern auch gegen "ausländische Spionage" richte. Es ging in der Tat darum, wirksam gegen die mannigfachen Versuche der totalitären Regime jener Zeit anzukämpfen, ihre Devisengesetzgebung, die oft auf Enteignung hinauslief, in der Schweiz zur Anwendung zu bringen und die Hand auf das in unsern Banken deponierte Vermögen der aus politischen oder rassischen Gründen verfolgten Personen zu legen. Der schweizerische Gesetzgeber wollte daher den Schutz der Persönlichkeit gegen Massnahmen verstärken, die unsere öffentliche Ordnung verletzen. Bankmoral und Bankrecht, wie die Schweizer sie für sich selbst entwickelt hatten, sollten auch für die Ausländer gelten.*
>
> *(Traduction de la citation : «En 1934, le législateur suisse a estimé nécessaire de renforcer par une disposition de droit pénal à l'article 47 de la loi sur les banques l'obligation de droit privé en vertu de laquelle le banquier est tenu au secret. Lors des délibérations sur cette disposition, on a fait remarquer qu'elle ne visait pas seulement ceux qui portent atteinte au secret bancaire, mais aussi l'«espionnage par l'étranger». Il s'agissait en fait de lutter contre les multiples tentatives des régimes totalitaires de l'époque d'appliquer en Suisse leur législation sur les changes, qui aboutissait souvent à une expropriation, et de s'approprier la fortune déposée dans nos banques de personnes poursuivies pour des motifs politiques ou racistes. C'est pourquoi le législateur suisse entendait renforcer la protection de*

---

40 Adrian Andermatt, Die Konzerninterne Bekanntgabe von geschützten Bankkundendaten ins Ausland - Eine strafrechtlich relevante Offenbarung im Sinne von Art. 47 BankG, GesKR 2007, 405, 409 (La divulgation de données bancaires protégées à l'étranger au sein d'un Groupe de sociétés – Une divulgation en droit pénal au sens de l'art 47 LB).

41 FF 1970 I 1144 ss., 1161.

la personnalité contre des mesures qui portaient atteinte à notre ordre public. L'éthique et le droit bancaires tels que les Suisses les avaient définis pour leur propre usage devaient également s'appliquer aux étrangers.»)

46 La vision historique de la volonté législative indique donc dans un premier temps, contrairement à la formulation, un traitement différent des mandataires à composante étrangère. Depuis lors, la LB a été révisée à plusieurs reprises et récemment adaptée à l'intérêt public dans une place financière internationale intégrée. Cette interprétation en termes de durée de validité doit être approfondie dans le cadre d'un examen systématique. Elle nous amène au fait que la volonté législative exprimée il y a 80 ans s'est estompée du point de vue d'aujourd'hui.

c) Interprétation systématique

47 Avec la législation la plus récente, la Suisse s'est considérablement distanciée des considérations du législateur en 1934:

48 Depuis 2017, les banques suisses communiquent aux autorités suisses des informations relativement détaillées sur leurs clients étrangers en participant à la norme mondiale sur l'échange automatique de renseignements sur les comptes financiers (EAR), afin que ces informations puissent ensuite être transférées de la Suisse à l'étranger. La Suisse souhaite donc maintenir l'ouverture vers le marché financier international («Level Playing Field», N. 14). Le Conseil fédéral en a soumis les bases à l'examen du Parlement en plusieurs itérations, de 2015 à 2018. La première loi EAR est en vigueur depuis 2017. Depuis 2018, la Suisse échange des renseignements sur les comptes financiers avec les États partenaires dans le cadre de l'EAR.

49 La Suisse a conclu un traité avec les États-Unis pour faciliter la mise en œuvre de FATCA («US Foreign Account Tax Compliance Act») et une loi suisse sur la FATCA correspondante a été adoptée. En vertu de l'accord FATCA, les banques suisses communiquent les informations relatives aux comptes de leurs clients directement aux autorités fiscales américaines avec l'accord des clients concernés. Si aucun consentement n'a été donné, un rapport anonyme et agrégé de certaines informations de compte est effectué à la place. Sur cette base, les autorités fiscales américaines peuvent alors exiger la divulgation de certains renseignements sur les clients et les comptes, si la convention de double imposition entre les États-Unis et la Suisse le prévoit.

50 Ces récents développements relativisent clairement l'importance de l'intention historique du législateur. Dans le cadre d'un système tel que l'EAR, les informations sur les clients des banques que les banques doivent communiquer de manière standardisée sont transmises à l'étranger *dans leur intégralité* et *sans condition préalable*, ce qui est important à plusieurs égards pour évaluer ici si un mandataire à composante étrangère peut être choisi par une banque suisse: l'intérêt de protection toujours poursuivi par le législateur en 1934 a de toute façon été surpassé par l'EAR, puisqu'il n'est plus nécessaire qu'un État étranger participant à l'EAR puisse accéder aux mêmes informations via le détour du mandataire (après avoir subi des procédures fondamentalement restrictives). Si des renseignements autres que ceux échangés en vertu de l'EAR devenaient importants pour l'État étranger, ce dernier pourrait communiquer directement avec le mandataire pour obtenir ces renseignements auprès des autorités judiciaires. Toutefois, même en Suisse, le secret bancaire ne protège pas contre l'accès des autorités judiciaires qui poursuivent des délits d'une certaine intensité. La Suisse fournira également à l'État étranger une entraide juridique à tout moment pour de

telles investigations complémentaires. Si des employés du mandataire devaient violer le secret, ils pourraient être poursuivis à l'étranger (selon la législation en vigueur) conformément à la loi en vigueur; selon l'avis, le délit commis à l'étranger pourrait également être poursuivi en Suisse.[42]

51 Ces considérations sont particulièrement importantes pour l'appréciation de l'art. 47 LB en tant que disposition pénale. L'art. 47 LB représente un renforcement juridique de la protection contractuelle du secret (N 9). Art. 47 LB est un délit officiel, qui exprime le devoir de l'État de poursuivre pénalement et de punir l'auteur d'une infraction. Il serait contradictoire que le même État, qui transmet des renseignements à l'étranger dans le cadre de l'EAR sans conditions préalables et de manière transversale sur l'ensemble du paysage bancaire (ou leurs clients), soumette à une responsabilité pénale les transmissions de données dans une mesure beaucoup plus étroite, qui sont stockées de manière restrictive sur des infrastructures informatiques techniquement sûres (sans l'exprimer expressément dans les éléments constitutifs de l'infraction objective). En raison de ces développements, l'élément d'interprétation historique subjectif (N 46) ne peut plus être décisif pour le résultat de l'élément d'interprétation.

52 Dans le cadre de l'interprétation systématique, il convient également de noter que l'opinion récemment exprimée dans le domaine du secret professionnel de l'avocat, selon laquelle le personnel auxiliaire étranger pourrait être légalement intégré dans la sphère de risque de l'avocat et qu'il ne constituerait pas une violation du secret professionnel si ce personnel auxiliaire étranger avait accès en texte clair à des informations soumises à une obligation de confidentialité.[43]

d) Interprétation téléologique

53 Pour l'interprétation téléologique, voir les remarques sous N 36. L'art. 47 LB a pour but de permettre à une banque de se positionner dans une économie basée sur la division du travail comme c'est nécessaire pour des raisons objectives. À cette fin, la banque devrait pouvoir intégrer les prestataires de services dans sa sphère de risque. Étant donné que le marché des services Cloud possède aujourd'hui un caractère international, l'argument téléologique conduit à continuer d'autoriser l'implication de mandataires étrangers.

54 En tout état de cause, il est clair que l'art. 47 LB n'est pas destiné à être une disposition pour la protection des fournisseurs nationaux de services Cloud. La disposition ne conviendrait pas à cette fin en tant que disposition pénale, une connotation correspondante devrait être rejetée dans le contexte de l'interprétation.

e) Conclusion

55 L'évaluation des éléments d'interprétation ci-dessus révèle une tendance claire à conclure que les banques peuvent également désigner des prestataires de services à composante étrangère comme mandataires au sens de l'article 47 LB.

---

42 Voir supra N 41.

43 SCHWARZENEGGER/THOUVENIN/STILLER, (note en bas de page 34), p. 21, 27s.

PARTIE 2 MISE EN ŒUVRE DE MESURES DE PROTECTION ADÉQUATES

I. Dérivations des considérations des éléments constitutifs de l'infraction, objectifs et subjectifs

A. Remarques préliminaires

56 Les considérations sur les éléments constitutifs de l'infraction, objectifs et subjectifs (voir supra N 15 ss.) ont démontré que l'article 47 LB doit être examiné comme un délit d'omission improprement dit d'une infraction commise par négligence (N 22). Tant du point de vue du statut de garante que de la négligence, la banque est tenue de faire preuve de la diligence requise lors du choix du fournisseur de services Cloud, d'anticiper les risques prévisibles et exiger du fournisseur de services Cloud de lui démontrer quelles mesures concrètes sont en place pour protéger les données des clients de la banque contre l'accès par des tiers non autorisés. Si, après un examen minutieux, la banque parvient à la conclusion que les mesures qui lui sont présentées ne conduisent pas, selon le déroulement prévisible des événements dans le cours normal des opérations, à une divulgation (même à l'égard des employés du fournisseur de services Cloud) ou si, sur cette base, elle intègre le fournisseur de services Cloud dans sa sphère de risque en tant que mandataire (l'accès en texte clair des employés du fournisseur de services Cloud étant également autorisé), elle ne contrevient ni sa qualité de garante, ni ses organes ou ses employés peuvent être punis pour des infractions commises par négligence.

57 La banque, qui assure une protection technique et organisationnelle appropriée, qui selon le cours ordinaire des choses empêche les tiers non autorisés d'avoir connaissance du secret dans le cours normal des opérations, ne peut pas, d'un point de vue évaluatif, violer le secret bancaire dans ce cas par les éléments constitutifs de l'infraction objective. Une **protection adéquate** signifie que des **précautions suffisantes** doivent être prises efficacement contre l'accès par des personnes non autorisées. De telles précautions sont suffisantes si selon le cours ordinaire des choses elles empêchent des personnes non autorisées de percevoir le contenu du secret («accès en texte clair») dans le cours normal des opérations.

58 La banque doit comprendre dans quelle mesure elle conserve le contrôle des données migrées vers les infrastructures informatiques externes au moyen de mesures documentées (obligation de protéger son propre périmètre, N 5); car la banque ne peut contrôler que ce qu'elle comprend.

59 Si la banque agit de la sorte, elle peut prouver qu'elle a rempli sa position de *garante contractuellement convenue* et qu'elle *n'agit pas de façon négligente*.

60 La banque doit s'assurer qu'elle dispose de structures internes et de personnel interne en place, tant dans le processus d'approvisionnement que dans le cours normal des opérations, pour garder le contrôle de l'échange avec le fournisseur de services Cloud. Cela peut signifier que le personnel interne doit occuper de nouveaux domaines de responsabilité et qu'il doit être formé pour acquérir les compétences nécessaires («Skill Shift»).

B. Dérogations aux considérations relatives à la désignation d'un mandataire

61 La loi ne précise pas spécifiquement comment un mandataire acquiert sa position – si cette position lui est attribuée par la loi à la conclusion du contrat ou si la banque doit l'intégrer dans sa sphère de risque par le biais d'un contrat. À notre avis, c'est ce dernier cas qui s'applique. Notamment la proximité de la notion fonctionnelle de personnel auxiliaire par rapport au consentement implicite (N 37 s.) montre clairement que ce n'est pas entièrement à la discrétion de la banque qu'il appartient de déterminer comment elle implique les tiers. La banque ne peut obtenir le privilège (N 39) que si elle fait du fournisseur de services Cloud un mandataire correctement en termes de contenu. En outre, la désignation formelle du mandataire au moyen d'un contrat répond à l'objectif de la sécurité juridique: En principe, chacun devrait pouvoir déterminer s'il peut faire l'objet d'une sanction pénale (ou si, en cas de violation de la confidentialité, il ne doit s'acquitter que de dommages-intérêts ou de pénalités contractuelles).

62 Notamment les lignes directrices suivantes sont importantes et la banque doit s'y conformer:

- Délimitation des sphères de risque: Le détenteur du secret (c'est-à-dire la banque) a le devoir direct de veiller à ce que le secret ne soit pas divulgué. Toute disposition qui expose le secret au risque d'être divulgué doit inciter la personne qui le détient à prendre des mesures pour le protéger. Si la banque prend de telles mesures, elle se comporte comme attendu du point de vue du client de la banque. Il est légal de faire confiance à d'autres personnes[44], y compris à des mandataires, dans sa propre sphère de risque. Pour ce faire, il faut toutefois définir la sphère de risque, ce qui exige des contrats correspondants clairement formulés.

- Un engagement contractuel est indispensable: Un contrat qui impose à des tiers des mesures techniques et organisationnelles suffisantes et dispose d'instruments contractuels de protection dans l'intérêt de la force exécutoire est indispensable.

- Considération des informations concernées: La banque devra protéger les informations particulièrement sensibles mieux que d'autres types d'informations. Dans le cas d'informations particulièrement sensibles, le cercle des personnes concernées devrait être plus étroit que dans le cas d'autres informations.[45]

63 Il découle de l'opinion exprimée ici que ce ne sont pas seulement des critères purement formels,[46] mais aussi des critères de contenu et des critères fonctionnels qui déterminent si un mandataire a été désigné de façon licite. Il ne suffirait pas que la banque soumette formellement le mandataire à «la responsabilité pénale de l'art. 47 LB». Les mesures prises doivent assurer que la banque instaure une protection adaptée à ses besoins. Cela exige également une compréhension approfondie de la part de la banque des processus (à assurer par le fournisseur de services Cloud) chez

---

44 SCHWARZENEGGER/THOUVENIN/STILLER, (note en bas de page 34), p. 21.

45 DAVID ROSENTHAL/YVONNE JÖHRI, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen (Commentaire sur la loi sur la protection des données et d'autres dispositions choisies), CO 328b N 57.

46 À juste titre dans la mesure où le TC ZH stipule dans son arrêt no UE140317 du 9 juillet 2015 au sens de l'article E 6: *«Allein die Tatsache, dass eine Person zur Bank ein Auftragsverhältnis unterhält, kann nicht genügen, um die Bank zur Weitergabe von Geheimnissen zu ermächtigen (vgl. Stratenwerth, a.a.O., N. 7 zu Art. 47 BankG).» (Traduction de la citation: «Le simple fait qu'une personne ait une relation contractuelle avec la banque ne peut suffire à autoriser la banque à divulguer des secrets (voir Stratenwerth, loc. cit., n. 7 sur l'art. 47 LB)».*

le fournisseur de services Cloud, car seulement quiconque comprend à quoi ressemblera le traitement de l'information chez le fournisseur de services Cloud peut le contrôler. À cette fin, le fournisseur de services Cloud doit documenter la banque de façon adéquate.

64 Si la banque mandate formellement le fournisseur de services Cloud de cette façon, il lui est possible d'accéder à des informations en texte clair sans que la banque ou ses organes et employés soient passibles de poursuites. La banque s'est alors acquittée de ses devoirs de diligence dont il est question sous N 22 ss.

C. Scénarios sans accès en texte clair

1. Remarques préliminaires

65 Tant que le fournisseur de services Cloud n'est pas officiellement impliqué en tant que mandataire, le fournisseur et ses employés sont également considérés comme non autorisés. Toutefois, cela ne signifie pas nécessairement que la banque ne sera pas en mesure d'utiliser les services Cloud, comme cela sera immédiatement démontré. Des services Cloud qui empêchent efficacement les situations de divulgation au moyen de mesures techniques et organisationnelles sont mis à la disposition de la banque. À cet égard, le scénario présenté sous ce point I.C ne diffère pas significativement des autres résultats présentés dans cette partie 2.

66 Si les données des clients des banques sont adéquatement protégées **contre l'accès par des tiers non autorisés** par les infrastructures informatiques du fournisseur de services Cloud, il n'y aura pas de divulgation relevant du droit pénal. Du point de vue de l'évaluation, il n'y a pas de divulgation si la banque, en tant que détentrice du secret, veille à ce que des mesures de protection correspondant à l'état actuel de la technique soient mises en place. Ce que cela signifie dans le contexte de services Cloud est décrit ci-dessous. Ce faisant, il convient d'envisager des scénarios d'utilisation et d'expliquer dans quelle mesure les variations possibles du modèle de service (IaaS, PaaS, SaaS) conduisent à des différenciations juridiques:

2. Analyse sous différenciation selon les modèles de service

a) Analyse lors de l'utilisation d'offres IaaS pures

67 Dans une offre IaaS pure, la banque utilise les infrastructures informatiques du fournisseur de services Cloud, principalement des bâtiments, des serveurs, des couches de virtualisation et des composants de stockage. Toutefois, ces ressources ne sont pas utilisées isolément, mais constituent les composants de base sur la base desquels des serveurs virtuels ou des machines virtuelles sont mis à la disposition de la banque.[47] La banque utilise ces machines virtuelles de la même manière qu'elle conservait et gérait avant dans ses propres locaux des composants de serveurs physiques avec des supports de données. L'expérience utilisateur de la banque ne diffère pas de manière significative de l'expérience utilisateur précédente (infrastructures informatiques de la banque).

---

47 Voir en annexe le terme «composante de base».

68 Les composantes de base utilisées par le fournisseur de services Cloud sont gérées chez lui de façon automatisée. Il s'agit de systèmes de contrôle permettant au fournisseur de services Cloud de gérer le grand nombre de ressources mises à la disposition de la banque à l'aide de méthodes uniformes (c'est-à-dire les mêmes que pour les autres clients) avec un effort raisonnable et un degré d'automatisation extrêmement élevé. En principe, il n'existe pas de support spécifique au client pour le bénéfice de la banque. Le fournisseur de services Cloud gère la solution d'automatisation centrale de sorte que les composants logiciels soient automatiquement mis à jour à tous les niveaux des infrastructures informatiques utilisées, ou une mise à jour pour tous les composants de base utilisés effectuée de façon uniforme (ou pour une sélection des composants de base définis selon des critères abstraits: numéro de version, âge du matériel, etc.). Le système de contrôle permet ainsi un contrôle plus efficace des actions pour maintenir et améliorer l'ensemble du système. La caractéristique centrale de cette procédure pour l'analyse juridique est que les ressources utilisées par le fournisseur de services Cloud ne sont pas gérées par des êtres humains dédiés à la banque, mais automatiquement et uniformément pour toute la clientèle. Cette approche peut être décrite comme «Hyperscale». Contrairement aux petites infrastructures informatiques, les services Cloud construits selon l'approche Hyperscale sont nécessairement anonymes. Alors que la solution d'automatisation centralisée est encore exploitée par les utilisateurs, ceux-ci contrôlent les critères de gestion plutôt que d'assumer des tâches de gestion «pour un seul client».

69 La gestion des infrastructures informatiques avec l'approche Hyperscale s'exprime dans des processus qui favorisent l'anonymat:

- des processus d'approbation garantissent qu'à aucun moment, un employé ne peut avoir un accès non autorisé à une composante de contrôle; l'accès à la composante de contrôle doit être approuvé par un responsable qui n'a que des fonctions d'approbation à cette fin, mais qui ne coopère pas avec la personne autorisée à y accéder. De tels processus d'approbation favorisent également l'anonymat au sein des équipes du fournisseur de services Cloud, minimisant, voire excluant, les conflits d'intérêts et la collusion au détriment d'un client particulier.

- Si l'accès est accordé à un employé, il ne l'est que pour la durée requise par l'employé pour le motif indiqué dans la demande d'autorisation – qui doit bien entendu être rendu plausible. C'est ce qu'on appelle l'accès «Just in Time». Les droits accordés sont limités et appropriés à l'objet de la demande d'accès («Just enough»).

- Dans le modèle IaaS, les mesures organisationnelles ne sont pas les seules utilisées. Une limitation technique des possibilités d'accès du personnel du fournisseur de services Cloud résulte de la fonctionnalité du logiciel de contrôle central. Elle est conçue pour mettre à jour les systèmes logiciels. Toutefois, il n'est pas prévu de permettre l'accès aux machines virtuelles des clients individuels (pour lesquelles d'autres systèmes sont requis et le consentement du client, comme indiqué dans le logiciel, est également requis).

- Toutes les mesures sont enregistrées dans des journaux (logs).

70 Dans le cours normal des opérations, cette méthode anonyme de mise à disposition et de gestion limite la probabilité globale qu'un employé d'un fournisseur de services Cloud puisse accéder à une

machine virtuelle de la banque et aux données qui y sont stockées. Les machines virtuelles sont protégées contre tout accès non autorisé par des mesures logicielles dans la couche de virtualisation.

71 De son côté, la banque est libre de définir la «vie intérieure» de la machine virtuelle de manière indépendante en utilisant l'approche IaaS: elle sélectionne la configuration logicielle spécifique (système d'exploitation et logiciel d'application) de la machine virtuelle et définit les modèles de données requis dans ce cadre. Si la banque perd les données d'accès à la machine virtuelle ou aux applications qui s'y exécutent, le fournisseur de services Cloud du modèle Hyperscale ne peut pas aider le client à prendre des mesures de restauration. Le client doit alors prendre lui-même ces mesures.

72 En outre, il convient de noter pour le modèle IaaS que l'ensemble du système est bien entendu coordonné par le fournisseur de services Cloud. Le fournisseur de services Cloud fournit les administrateurs au plus haut niveau.[48] Si un employé du fournisseur de services Cloud doit accéder au système et être en mesure de visualiser les données du client pendant cet accès, il doit être autorisé par l'administrateur du client (un processus qui est visualisé et sécurisé au moyen de mesures techniques et organisationnelles). Dans le système global, l'administrateur du client est, pour ainsi dire, l'administrateur du niveau le deuxième plus haut[49] (l'employé de support activé en plus par le client aurait le rôle d'un utilisateur à court terme ou d'un administrateur subalterne au troisième niveau).[50]

73 La description d'un modèle IaaS ci-dessus en aucun cas n'est pas complète. Toutefois, les explications doivent démontrer que, selon le modèle de service et au moyen d'une multitude de mesures interdépendantes de nature technique et organisationnelle, la probabilité et, dans une large mesure, la possibilité pour les employés de dans le cours normal des opérations accéder aux machines virtuelles du client et donc aux données stockées sont réduites, voire exclues. Le degré élevé d'automatisation et d'anonymat inhérent à l'approche Hyperscale offre donc à la banque, en tant que client, une protection naturelle contre l'accès non autorisé en texte clair aux données bancaires des clients par les employés individuels du fournisseur de services Cloud.

74 Si le fournisseur de services Cloud est en mesure de documenter de manière plausible une combinaison de mesures aussi efficace, la banque peut prouver que son choix (p. ex. «modèle IaaS pur») en combinaison avec les mesures documentées conduit à une protection contre l'accès non

---

48 Rôle d'administrateur du plus haut niveau: Ce terme est utilisé pour des raisons d'intelligibilité, mais il est imprécis d'un point de vue technique. Il s'agit plutôt d'une séparation des tâches où le fournisseur de services Cloud gère les composants de base sous-jacents et n'a rien à voir avec les machines virtuelles. L'administrateur du fournisseur de services Cloud aurait la possibilité de démarrer et d'arrêter une machine virtuelle définie sans y avoir accès. La possibilité d'arrêter une machine virtuelle est limitée aux cas urgents où la machine virtuelle affectée tourne en dehors du cours normal des opérations et où cet état affecterait la stabilité des machines virtuelles fonctionnant dans le même environnement.

49 La terminologie, en revanche, n'est à nouveau pas techniquement exacte. Dans la pratique, il s'agit de ségrégation. Les administrateurs du client peuvent être appelés administrateurs VM ou administrateurs IaaS.

50 Si le fournisseur de services Cloud doit distribuer automatiquement certains progiciels sur la machine virtuelle du client pour des raisons techniques, par exemple pour le «patching» de la couche logicielle, cela peut être réalisé au moyen d'entrées standardisées dans le système d'autorisation du client. Le concept de l' «Admin Eligible », par exemple, est connu pour de tels accès sans consultation des données. Il serait toutefois excessif d'approfondir ce concept ici.

autorisé si prévisible que l'accès en texte clair peut être raisonnablement exclu lors du fonctionnement normal de la solution.

75 Le fait que le fournisseur de services Cloud ait un accès direct à la machine virtuelle du client peut techniquement être exclu. Théoriquement, cependant, il n'est pas exclu que le fournisseur de services Cloud puisse accéder au fichier de stockage crypté[51] de la machine virtuelle (le fournisseur de services Cloud fournit l'administrateur du niveau le plus haut, N 72). Le fait qu'il décrypte ce fichier en utilisant ce que l'on appelle la «force brute» ne peut pas être techniquement exclu à cent pour cent. Cependant, cette possibilité est si marginale qu'elle ne peut être sérieusement décrite comme un danger réaliste. Toutefois, étant donné que des mesures techniques et organisationnelles sont en place pour garantir qu'un tel accès n'a pas lieu dans le cours normal des opérations, le modèle IaaS ne donne pas lieu à des sanctions pénales si une banque migre des données dans les infrastructures informatiques du fournisseur de services Cloud. Cette conclusion se fonde sur la jurisprudence la plus récente du Tribunal fédéral (selon laquelle seul l'accès effectif compte, voir ci-dessus la N 17).

b) Analyse lors de l'utilisation d'offres PaaS pures

76 Une offre PaaS diffère d'une offre IaaS par le fait que le client ne gère pas les machines virtuelles lui-même. C'est le fournisseur de services Cloud qui gère les machines virtuelles, y compris le système d'exploitation et les logiciels de plate-forme tels que les logiciels de base de données et autres, qui sont entièrement exploités par le fournisseur de services Cloud. Les composantes techniques de base utilisées dans le modèle PaaS ne sont pas différentes de celles utilisées dans le modèle IaaS. Cependant, la mise à disposition diffère:

- avec le modèle IaaS, un client «réserve» certaines ressources à partir de son «Tenant». Par la suite, ces ressources sont enregistrées pour le client dans son système d'autorisation, c'est-à-dire, dédié (au moyen de définitions logiques dans les systèmes d'identité et les systèmes réseau). Comme déjà décrit, le fournisseur de services Cloud fournit les administrateurs du plus haut niveau dans le système global, tandis que le client fournit les administrateurs du deuxième plus haut niveau (N 72).

- Dans le modèle PaaS, un service est d'abord configuré en tant que produit standard par le fournisseur de services Cloud. Cela signifie que le fournisseur de services Cloud fournit également les administrateurs du deuxième plus haut niveau (outre les administrateurs au plus haut niveau). Si le client enregistre de tels produits standard à partir de son «Tenant», des entrées sont générées dans son système d'autorisation qui utilisent des méthodes logiques pour garantir que le stockage des données du produit standard soit lié au produit standard d'une manière unique et exclusivement pour lui (et non pour un autre client). L'administrateur du client devient l'administrateur du troisième plus haut niveau du système global. Si le client demande un support dédié auprès du fournisseur de services Cloud basé sur le «Tenant»

---

51 Dans une machine virtuelle, les données sont stockées dans un format spécifique (VHDX, VMDK, etc.) et sont techniquement protégées contre l'accès en texte clair.

du client, l'administrateur du client autorisera l'employé de support de consulter le «Tenant» du client.

77 Le droit d'utilisation du client (c'est-à-dire de la banque) est donc également déterminé dans le modèle PaaS par la définition du «Tenant». Le mot-clé central de la manière dont le client conserve le contrôle de ses données dans un environnement PaaS est «Tenant Isolation» (ou «Tenant level isolation» ou similaire). Toutefois, la présentation dans N 76 montre que des mesures organisationnelles sont de plus en plus mises en œuvre pour protéger le stockage des données du client contre l'accès des employés du fournisseur de services Cloud. En ce qui concerne la question, déterminante en droit pénal, de savoir si une divulgation pertinente d'informations confidentielles se produit, rien ne change en conséquence – pour autant que des méthodes suffisantes pour protéger contre un accès non intentionnel à la mémoire des données de la banque puissent être prouvées dans le système global. La conclusion selon N 75 peut donc également être transférée au modèle PaaS.

c) Analyse de l'utilisation des offres SaaS sans composante étrangère (ou offres IaaS ou PaaS complétées par des composantes SaaS)

78 Avec un modèle SaaS, le contrôle de l'ensemble du système s'approche encore plus du fournisseur de services Cloud. Bien que le modèle IaaS dispose encore d'une variété de mécanismes de protection qui sont intrinsèquement dus à des problèmes d'architecture technique, ces mécanismes de protection technique sont largement omis. En d'autres termes, les mesures de protection organisationnelles dans le modèle SaaS deviennent encore plus importantes. Les mécanismes de protection impliqués ne peuvent être décrits ici en termes abstraits, car dans les modèles SaaS, les mécanismes d'action concrets peuvent grandement différer selon le client. Le point essentiel est que la banque peut confirmer après analyse de ces mécanismes (qui, comme on l'a vu, seront principalement de nature organisationnelle) dans le cours normal des opérations, avec une fiabilité suffisante, que les employés du fournisseur de services Cloud ne disposeront d'aucun accès non autorisé en texte clair aux informations protégées de la banque ou de ses clients.

3. Conclusion

79 Les architectures des services Cloud matures, fortement orientées vers la gestion anonyme des composants de base, permettent l'utilisation d'infrastructures informatiques tierces sans accès au texte en clair (divulgations) dans le cours normal des opérations. Si la banque s'assure que des mesures techniques et organisationnelles appropriées sont mis en place pour se protéger contre les divulgations, elle peut utiliser ces services Cloud sans enfreindre l'art. 47 LB – même si elle ne désigne pas le fournisseur de services Cloud comme mandataire. Ces services Cloud sont des extensions du périmètre physique et logique de la banque (voir N 5), pour ainsi dire, et il n'y a pas d'extension du périmètre des ressources humaines.

II. Mesures de garantie (Fallback): Protection contre l'«Incidental Access» pur

80 Ci-dessous, on traite la question de savoir si un employé du support du fournisseur de services Cloud peut avoir accès à des informations protégées en texte clair au cas par cas dans des situations de support si le fournisseur n'a pas été désigné comme mandataire (sinon, les accès du

support sont privilégiés dès le départ). Un tel accès à des données protégées peut se produire dans des cas suivants:

a. Incident: La banque a un problème *dans* son «Tenant», pour la résolution duquel elle a besoin d'aide; elle veut faire appel à un employé du fournisseur de services Cloud.

b. Maintenance: La banque s'appuie sur le fabricant de certains composants logiciels pour effectuer des travaux de maintenance logicielle chez son «Tenant». La banque souhaite qu'un employé du fournisseur de services Cloud donne de l'assistance directement au fabricant des composants logiciels.

c. Support: La banque souhaite être soutenue dans la réalisation des travaux de maintenance du logiciel pour lesquels elle désire faire appel à un collaborateur du fournisseur de services Cloud.

81 Le fait que la banque ait besoin du fournisseur de services Cloud ou de ses employés dans de telles situations est pratiquement impossible, en tout cas, très rare. Néanmoins, la possibilité qu'une banque puisse encore vouloir faire appel au fournisseur de services Cloud sera évaluée ci-dessous sous l'aspect juridique. Il faut cependant être conscient qu'il s'agira de scénarios extrêmement rares.

82 Le «Cloud» n'existe pas (N 67 ss.). Les remarques ci-dessus l'ont déjà démontré. Une différenciation supplémentaire selon les modèles de service n'est pas effectuée à ce stade, seulement la comparaison entre une solution IaaS et SaaS.

1. Dans le modèle IaaS

83 Par exemple, si un employé du fournisseur de services Cloud a accès à distance à la machine virtuelle de la banque (parce que la banque l'y autorise) et que l'employé de support y accède en texte clair dans ce contexte, la banque doit surveiller les actions de l'employé de support dans la machine virtuelle. La banque n'est pas autorisée à laisser au personnel de support du fournisseur de services Cloud le contrôle de l'écran que dans des cas exceptionnels (uniquement si nécessaire: «need to know»). En principe, il n'est même pas nécessaire que l'employé du fournisseur de services Cloud effectue lui-même ce contrôle. Au contraire, l'employé de la banque pourra mettre en œuvre lui-même le contrôle par le biais d'instructions vocales de l'équipe de support. Si, dans des cas exceptionnels, il est nécessaire que l'employé du fournisseur de services Cloud prenne temporairement le contrôle d'une machine virtuelle de la banque, l'employé de la banque doit pouvoir interrompre ou arrêter temporairement les processus à tout moment. L'employé de banque ne doit dans ce cas jamais quitter l'écran.

84 En cas d'un support, il existe également un nombre limité de cas imaginables dans lesquels l'employé du fournisseur de services Cloud doit être en mesure de consulter les données des clients. Ce n'est que dans ce cas que la divulgation aura lieu. Toute divulgation est en principe prescrite. Par conséquent, la banque doit généralement s'abstenir de présenter de telles demandes de support.

85 Lorsque de telles demandes de support de la part de la banque divulguant des données de clients de la banque deviennent néanmoins nécessaires, il est généralement possible pour la banque soit de mettre en place un mécanisme d'atténuation, soit d'effectuer un «Workaround» (solution de contournement).

86 Les possibilités des Workarounds sont les suivantes:

a. La banque fait appel à un mandataire local, le désigne formellement comme mandataire et lui demande de réaliser cette tâche très particulière (éventuellement avec le support hors ligne du fournisseur de services Cloud).

b. La banque anonymise les données du client de la banque ou les supprime temporairement du système.

c. La banque crée temporairement une copie numérique identique de la machine virtuelle sans données client et visualise le problème au personnel de support du fournisseur de services Cloud sur cette base.

87 Les combinaisons de mesures peuvent être considérées comme des mesures d'atténuation. Si un employé de support du fournisseur de services Cloud doit effectivement inspecter les données, il peut être intégré à l'autorité de contrôle de la banque avec des règles de secret particulièrement strictes (par exemple, avec des pénalités contractuelles sensibles). Par conséquent, l'employé de support devient formellement le mandataire de cette action concrète isolée. Dans le cas contraire, une solution doit être trouvée au cas par cas pour permettre un contrôle efficace de la banque.

88 Enfin, des scénarios sont envisageables qui pourraient ouvrir une possibilité de justification dans des cas individuels, tels que l'état d'urgence ou des cas mineurs absolus. De tels scénarios ne devraient toutefois être envisagés et évalués avec beaucoup de prudence que dans le cadre d'une analyse des risques effectuée à l'avance. Ils peuvent être justifiés s'ils constituent une exception absolue. S'il s'agissait d'événements réguliers, ils devraient probablement être considérés comme appartenant au cours normal des opérations. Cela conduirait alors à des évaluations différentes.

89 En résumé, les scénarios (extrêmement rares) décrits au début de cet avis dans un modèle IaaS, où un «Incidental Access» pourrait se produire, donnent lieu à des constellations tellement nombreuses sans divulgation ou avec la possibilité d'une justification, que le cas d'un support (et les autres scénarios d'un «Incidental Access») ne devrait pas constituer une raison pour interdire à la banque d'utiliser a priori les services Cloud globalement et intégralement.

2. Dans le modèle SaaS

90 Pour les composants SaaS, il n'est généralement plus possible de faire la différence entre les machines virtuelles, car ces machines virtuelles ne sont généralement pas affectées à un seul client. L'analyse se réfère ici exclusivement aux *Tenants*, c'est-à-dire aux zones d'accès logiquement séparées, fournies au client à travers plusieurs machines virtuelles. Ici aussi, on peut distinguer si le fournisseur de services Cloud doit travailler à l'intérieur ou à l'extérieur du «Tenant» pour effectuer le travail mentionné dans N 80.

91 Dans le modèle SaaS, le fournisseur de services Cloud s'«approche» davantage du «Tenant» utilisé par le client que dans le contexte IaaS ou PaaS. Les architectures logicielles sont également mises en place différemment et séparent souvent moins précisément les ressources utilisées par le client de celles gérées entièrement par le fournisseur de services Cloud.

92 En tout état de cause, la capacité de la banque à stocker des informations sur ses clients dans les architectures informatiques du fournisseur de services Cloud de sorte que ce dernier ne puisse pas les percevoir dès le départ dépend fortement de la conception de la solution que le fournisseur de services Cloud a mise en place. Ce n'est que si le fournisseur de services Cloud s'est assuré sur le plan architectural que les «Tenants» installés dans le modèle SaaS soient séparés des composants de base nécessaires à la gestion des applications et à la maintenance logicielle que le fournisseur de services Cloud peut s'en servir et établir des règles organisationnelles claires pour empêcher ses employés d'accéder au «Tenant» de son client. Le choix des modèles SaaS exige donc une sélection encore plus rigoureuse de la part du client. Les exigences envers le service d'approvisionnement interne de la banque sont de plus en plus élevées pour de tels modèles. Cependant, si le fournisseur de services Cloud a pris en charge ces architectures informatiques, il peut également proposer au client des processus qui réduisent ou excluent de manière proactive les points de contact avec le «Tenant» du client.

> *Quelques fournisseurs individuels de Cloud, par exemple, ont mis en place des mécanismes de protection spéciaux de nature organisationnelle pour les travaux qui impliquent le risque que le «Tenant» du client soit accessible. Un exemple bien connu est un modèle de processus Microsoft appelé «Customer Lockbox» (une mesure purement organisationnelle). En vertu de ce régime, un employé de support ne peut avoir accès au «Tenant» en question que par le biais d'instructions internes après avoir suivi une certaine procédure. Dans les documents marketing, Microsoft s'attend à ce qu'il ne soit pratiquement jamais nécessaire qu'elle ait accès au «Tenant» ou aux données stockées dans celui-ci (les cas exceptionnels pour lesquels le client est informé de manière proactive et peut donner son consentement préalable seraient négligeables).*

93 Si l'architecture informatique ne dispose pas des bases nécessaires pour de telles mesures organisationnelles, de nombreux fournisseurs de services Cloud construisent un système qui utilise des journaux d'accès pour vérifier la mesure dans laquelle un employé accède à un «Tenant» sans en avoir besoin («need to know»).[52] Cette protection a un effet proactif en ce sens que les employés savent qu'on vérifie s'ils effectuent un accès non autorisé et qu'ils doivent s'attendre à des sanctions sévères en cas d'abus. Les journaux permettent également de surveiller rétrospectivement le comportement du fournisseur de services Cloud.

94 Conclusion: Des configurations techniques et des dispositifs organisationnels sont possibles, ce qui exclut une divulgation lors d'actions opérationnelles dans une mesure suffisante également avec des modèles SaaS.

---

52 Si le fournisseur de services Cloud se laisse auditer, ces journaux d'accès sont d'une importance capitale. Les auditeurs procèdent à l'audit selon des normes internationalement reconnues (par exemple, l'International Standard on Assurance Engagements, ISAE, administrée par l'International Federation of Accountants, IFAC), les normes sur la fiabilité des informations financières (ISAE 3402) étant distinguées des normes sur l'intégrité et la protection des autres informations (ISAE 3000) (semblable à la distinction SOC 1 contre SOC 2, où «SOC», qui signifie «Service Organisation's Controls»). Lors de ces contrôles, certains journaux d'accès sont souvent complètement audités, ce qui permet au moins de contrôler ultérieurement la fiabilité des mesures prises par le fournisseur de services Cloud. On distingue les audits ponctuels (type I, type 1 ou, dans d'autres normes, également de type A; «instantanés») et ceux qui s'étendent sur une période plus longue, généralement de six mois (type II, type 2 ou, dans d'autres normes, aussi le type B).

3. Résultat

95 Les considérations qui précèdent montrent que soit la banque ne sera pas en mesure de coopérer avec le fournisseur de services Cloud (travaux de maintenance dans le modèle IaaS et PaaS pour ses propres applications) pour le support éventuellement demandé, soit qu'elle pourra mettre en place divers dispositifs de sécurité pour protéger les intérêts de l'intégrité de la banque et de ses clients dans le cours normal des opérations.

96 Dans le cadre des travaux de maintenance, du traitement des incidents et des demandes de support, il n'y a pas a priori une interdiction pour la banque d'utiliser des services Cloud construits selon l'état actuel de la technique de fournisseurs de services Cloud fiables et soigneusement audités.

CONSÉQUENCE: LES BANQUES SUISSES SONT HABILITÉES À UTILISER LES SERVICES CLOUD MATURES

Les considérations sur la relation contractuelle entre la banque et le client de la banque (N 7s., N 11 ss. et N 13), la dogmatique générale du droit pénal (art. 11 CP, N 22 et surtout N 26 et art. 12 CP, N 28), les considérations constitutionnelles (N 12), la jurisprudence récente (N 17) et la doctrine unanime conduisent tous au même résultat: une banque doit être autorisée à utiliser les infrastructures informatiques si celles-ci sont protégées par des mesures adéquates (pour l'état actuel de la technique, voir N 26). L'exploitant de ces infrastructures informatiques n'est pas pertinent en soi.

L'avis juridique montre ainsi que les banques suisses peuvent utiliser les services Cloud si elles choisissent des fournisseurs de services Cloud fiables qui fournissent une infrastructure informatique mature dans le cadre d'un processus d'approvisionnement prudent. Grâce à des mesures techniques, organisationnelles et, dans certains cas, contractuelles, ces fournisseurs de services Cloud peuvent assurer une protection suffisante des informations secrètes.

Tant que le fournisseur de services Cloud s'assure que les informations ou les données sous-jacentes que la banque a migrées vers l'infrastructure informatique du fournisseur Cloud peuvent être accédées nulle part de manière non autorisée et si cela est garanti à tout moment, la banque ne viole pas les éléments constitutifs de l'infraction objective de l'art. 47 LB – même sans désigner le fournisseur de services Cloud comme mandataire.

Les fournisseurs de services Cloud peuvent être désignés comme mandataires de la banque. Dans la pratique, il ne faut toutefois pas surestimer l'importance de l'intégration du fournisseur de services Cloud en tant que mandataire au sens de l'article 47 LB. Si la banque comprend en détail comment les processus névralgiques sont mis en œuvre chez le fournisseur de services Cloud, elle constatera dans la plupart des cas qu'il n'y aura pas de divulgations significatives – ce qui rendra superflue l'implication du fournisseur de services Cloud en tant que «mandataire». Toutefois, ce contrôle est nécessaire sur la base de l'art. 11 al. 2 CP et de l'art. 12 al. 3 CP, même si la banque désigne le fournisseur de services Cloud comme mandataire.

* * *

ANNEXE: TERMES UTILISÉS

Les termes suivants sont utilisés de façon constante dans le présent avis juridique:

Fournisseur de services Cloud signifie fournisseur de services informatiques basés sur le Cloud. Cela inclut toutes les profondeurs d'intégration de la solution de Cloud, de IaaS à PaaS en passant par SaaS.

Composante étrangère fait référence soit aux relations internationales du fournisseur de services Cloud (domicile légal, etc.), soit à celles du service Cloud (localisation du centre de données, domicile des employés ou des tiers mandatés, etc.). Par exemple, une composante étrangère existe si (i) le fournisseur de services Cloud a son domicile légal à l'étranger; (ii) le fournisseur de services Cloud exploite ou laisse exploiter des infrastructures informatiques à l'étranger ou (iii) si le fournisseur de services Cloud emploie du personnel ou des sous-traitants à l'étranger.[53]

Banque comprend les personnes morales soumises à la Loi sur les banques en vertu de l'art. 1a, de l'art. 1*b* et de l'art. 2 LB.

Composants de base est un terme qui exprime le fait que les infrastructures informatiques du fournisseur de services Cloud ne constituent pas seulement le «Tenant», mais font aussi l'objet des services d'exploitation du fournisseur de services Cloud et sont gérés par le fournisseur de services Cloud en arrière-plan via des systèmes de contrôle.

Service Cloud ou solution Cloud constitue l'ensemble des services avec lesquels un fournisseur de services Cloud accorde à une banque l'utilisation de certaines infrastructures informatiques sous une forme standardisée, automatisée, évolutive et non dédiée via des réseaux de données. Les services Cloud peuvent soulager les banques de la nécessité d'exploiter leurs propres centres de données, matériels et logiciels serveurs (Infrastructure as a Service, **IaaS**), ou elles peuvent aider les banques à éviter d'avoir à exploiter et maintenir elles-mêmes certains logiciels (logiciels d'exploitation ou applications utilisateur) (Platform as a Service, **PaaS**, ou Software as a Service, **SaaS)**. L'e service Cloud désigne ici le terme familier «**Public Cloud**», qui signifie que les composants de base du fournisseur de services Cloud ne peuvent d'une part pas être utilisés individuellement et exclusivement («dédiés») par un client; d'autre part, l'option utilisateur offerte par un «Tenant» est spécifique au client et délimitée des autres clients («isolation»), et rendue possible par la technologie réseau.

Infrastructures informatiques désignent l'ensemble des bâtiments, du matériel, des logiciels, de la technologie réseau, etc. qu'un fournisseur de services Cloud utilise pour fournir un service Cloud.

Accès en texte clair désigne le processus par lequel une personne peut reconnaître, lire et mémoriser ou transmettre la signification d'un signe qu'elle voit sans avoir besoin d'autres aides. En revanche, le *simple accès* à l'emplacement de stockage des données ne constitue pas un accès en texte clair. Quiconque est autorisé à visiter une salle de serveurs et passe devant les supports de données dans le

---

[53] Pour cette catégorie (personnel ou sous-traitants), la composante internationale existe si l'accès au service Cloud peut être obtenu depuis l'étranger.

couloir entre les serveurs a évidemment accès aux données (plus précisément à l'emplacement du stockage des données). Même s'il le fait sans surveillance, il n'a pas encore pris connaissance des contenus stockés sur les supports de données. Si le visiteur quitte à nouveau la salle des serveurs sans avoir accès aux supports de données, rien n'est arrivé en ce qui concerne le secret à garder. De même, on ne parle pas d'accès en texte clair lorsqu'une personne a besoin d'un outil technique pour pouvoir en reconnaître le sens, etc. Un tel outil pourrait être un écran connecté à un dispositif de traitement de données, ou une application qui accède à une base de données et rend les informations stockées dans la base de données lisibles pour l'utilisateur. Ce terme est important pour la compréhension des obligations de secret. Le droit suisse ne prévoit toutefois pas de terminologie appropriée pour distinguer les informations reconnaissables par l'homme de la mise en forme technique qui ne peut être interprétée que par des machines, mais ne peut pas être reconnue par l'homme sans moyens auxiliaires. C'est pourquoi nous utilisons ici ce terme familier.

Cours normal des opérations[54] signifie que le service Cloud est exploité comme prévu par le fournisseur de services Cloud (par opposition à des situations extraordinaires qui ne peuvent pas être attribuées au cours normal des opérations, telles que: la faillite[55] du fournisseur de services Cloud; l'accès par les autorités[56] au service Cloud; l'accès par des criminels au service Cloud).

Tenant est l'environnement d'utilisation propre au client mis à la disposition de la banque et, par conséquent, une zone d'accès exclusivement mise à la disposition de la banque et de ses employés au moyen de la technologie réseau. Un «Tenant» est généralement rendu possible à travers plusieurs composantes de base; l'affectation exacte d'un «Tenant» à une certaine composante de base est variable en termes de temps; en termes d'incidence, une affectation serait possible seulement à un moment précis («Snapshot»), mais cela nécessiterait un effort démesuré.

* * *

---

54 Cette distinction se justifie par le fait qu'une banque n'a besoin d'examiner les risques juridiques liés à la divulgation que dans la mesure où elle peut les contrôler. Toutefois, dans la mesure où certains risques peuvent être prévus de manière abstraite, ils peuvent déclencher des obligations d'information envers les clients des banques.

55 La banque doit planifier soigneusement ce scénario et surveiller le fournisseur de services Cloud en ce qui concerne le risque d'insolvabilité. Cela inclut l'obligation de la banque de maintenir une interaction étroite avec le responsable des comptes clés du fournisseur de services Cloud et d'examiner régulièrement les états financiers de ce dernier. La banque doit également être en mesure de mesurer sa planification de la continuité des opérations (Business Continuity) par rapport à de tels scénarios (pour permettre un rétro-sourcing rapide et une suppression immédiate des données). Par exemple, un plan d'urgence doit être mis en place, en vertu duquel la banque supprime les données secrètes immédiatement et directement via le panneau d'administration du portail client dès que la banque a connaissance de la faillite du fournisseur de services Cloud – avant même que l'administrateur judiciaire éventuellement désigné ne bloque l'accès aux infrastructures informatiques du fournisseur de services Cloud.

56 Une autorité de poursuite pénale exige que la banque ou le fournisseur de services Cloud lui donne accès aux données d'un client de la banque (ou aux données de la banque). Très peu d'auteurs discutent du risque de l'accès d'autorités judiciaires étrangères d'une manière appropriée, c'est-à-dire sans commenter les questions telles que la loi CLOUD, l'US PATRIOT Act et les règlementations similaires du droit pénal de gouvernements étrangers. Le risque d'accès des autorités nationales doit également être traité comme une situation qui ne peut pas être attribuée au cours normal des opérations. L'accès par une autorité suisse peut avoir des effets similaires ou même plus dramatiques sur les clients des banques que l'accès par une autorité judiciaire étrangère. Bien sûr, cela peut aussi avoir lieu dans l'autre sens. En règle générale, la banque ne connaît pas l'exposition au risque du client de la banque à cet égard. Toutefois, la banque doit comprendre la probabilité et les circonstances dans lesquelles une autorité peut accéder à ses données (indépendamment de l'utilisation des services Cloud).