Haut Comité Juridique
de la Place financière de Paris

RAPPORT SUR LE SECRET BANCAIRE

du Haut Comité Juridique
de la Place Financière de Paris

Le 6 juillet 2020

9 rue de Valois 75001 Paris - Tél.: 33 (0)1 42 92 20 00 - hautcomite@hcjp.fr - www.hcjp.fr

RAPPORT SUR LE SECRET BANCAIRE DU HAUT COMITÉ JURIDIQUE DE LA PLACE FINANCIÈRE DE PARIS

Les évolutions de la pratique de l'activité bancaire qui, notamment, a de plus en plus recours à la sous-traitance, mais également l'apparition de nouvelles réglementations[1] suscitent des interrogations nouvelles sur la portée du secret professionnel auquel les établissements de crédit[2] sont notamment tenus (ci-après « le secret bancaire »). Ainsi, le Haut Comité Juridique de la Place Financière de Paris (HCJP) a constitué un groupe de travail[3] chargé d'examiner si des modifications au régime actuel, légal et jurisprudentiel, en matière de secret bancaire apparaissent souhaitables.

Après un rappel du droit positif en la matière (objet, champ d'application, exceptions, sanctions - Section I/), le présent rapport détaille les problématiques auxquels les établissements sont aujourd'hui confrontés, tant au regard de la jurisprudence (notamment en matière de droit de la preuve – Section II/) que des évolutions de la pratique ou de l'organisation des établissements (Sections III/ et IV/) ou des réglementations récentes (RGPD, DSP2 - Section V/). Le groupe de travail s'est par ailleurs attaché à formuler des recommandations pour pallier les difficultés rencontrées.

***

Lors de sa séance plénière du 06 juillet 2020, le HCJP a approuvé le présent rapport et a fait siennes ses conclusions.

***

[1] En particulier le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données, ou « RGPD », et la Directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, dite Directive Service de Paiement II ou « DSP2 ».

[2] Les travaux du groupe de travail se sont concentrés sur le secret professionnel applicable, en vertu des articles L.511-33 et L.522-19 du Code monétaire et financier, aux établissements de crédit, aux sociétés de financement, aux organismes mentionnés aux 5 et 8 de l'article L.511-6 du Code monétaire et financier ainsi qu'aux établissements de paiement.
Si les travaux n'ont en revanche pas spécifiquement porté sur le secret professionnel applicable aux prestataires de services d'investissement (Titre III du Livre V du Code monétaire et financier) régi par l'article L.531-12 du même code, les dispositions de cet article sont très proches de celles figurant aux articles L.511-33 et L.522-19, de telle sorte que les recommandations formulées au sein du rapport apparaissent, en grande partie, transposables au sein de l'article L531-12 du Code monétaire et financier.

[3] La composition du groupe de travail figure en Annexe n° 1.

SYNTHÈSE DES CONCLUSIONS DU GROUPE DE TRAVAIL

Le devoir de discrétion du banquier vis-à-vis des affaires de son client est un principe ancien et majeur de la profession bancaire. Le banquier tient, dans ses relations avec son client, un rôle de « confident nécessaire » au regard des informations d'ordre financier et patrimonial, mais également d'ordre personnel, qu'il est amené à connaître le concernant. Le secret constitue, dans ces conditions, un élément essentiel de cette relation et la sauvegarde de l'intérêt privé de son client fonde en grande partie l'obligation de discrétion auquel le banquier doit rester tenu à son égard.

Le secret bancaire auquel sont assujettis, notamment, les établissements de crédit[4] (ci-après désignés « les établissements assujettis ») n'a été légalement consacré dans le droit français qu'en 1984[5]. La dernière réforme du secret bancaire date quant à elle de 2008 : la loi de modernisation de l'économie[6] a codifié la faculté pour son créancier d'y renoncer[7] et a élargi, significativement, la liste des exceptions légales au secret.

À l'issue de ses travaux, le groupe de travail a constaté que les contours de cette obligation, dont le périmètre est très large, demeurent complexes à appréhender du fait d'une multitude d'exceptions disséminées dans la réglementation et d'évolutions jurisprudentielles régulières. L'appréhension du périmètre précis d'application du secret bancaire demeure source d'insécurité juridique, tant pour les personnes protégées que pour les établissements assujettis (et les personnes physiques astreintes au secret) qui restent exposés à des sanctions pénales, certes peu prononcées, mais particulièrement lourdes. Cette difficulté de lecture de la réglementation en matière de secret bancaire et cette insécurité juridique participent au manque d'attractivité du droit français.

S'agissant de la pénalisation du secret bancaire français, il convient de noter qu'il s'agit d'un principe qui n'est pas partagé par la majorité des autres pays de l'Union européenne (*cf. Annexe n° 2*). À ce titre, le groupe de travail s'est interrogé sur la question de sa dépénalisation mais a néanmoins considéré que cette question ne relevait pas du périmètre de sa mission, le secret bancaire s'intégrant dans le régime plus large du secret professionnel applicable à d'autres professions, notamment celui des avocats ou des médecins.

---

[4] Les articles L.511-33 et L.522-19 du Code monétaire et financier s'appliquent aux établissements de crédit, aux sociétés de financement, aux organismes mentionnés aux 5 et 8 de l'article L.511-6 du Code monétaire et financier ainsi qu'aux établissements de paiement.

[5] Par la loi n° 84-46 du 24 janvier 1984 dite « loi bancaire ». Cette loi a notamment consacré le caractère pénal du secret bancaire par renvoi aux dispositions du Code pénal.

[6] Loi n° 2008-776 du 4 août 2008.

[7] Le principe de la nécessité du consentement du client à la levée du secret était jusqu'alors, uniquement posé par la jurisprudence.

L'organisation des établissements a par ailleurs fortement évolué au cours de ces dix dernières années. Avec le recours croissant aux prestataires informatiques, la diversification de leurs activités, la filialisation et la spécialisation des entités au sein de groupes bancaires de plus en en plus larges et transfrontières, la circulation de la donnée (notamment personnelle) et de l'information au sein des organisations est devenue indispensable à la réalisation de leur activité et à la délivrance d'un service de qualité aux clients. Dans ce contexte, la complexité du régime juridique du secret bancaire est accrue par un texte dont la rédaction apparaît parfois imprécise ou qui n'est plus adaptée à l'organisation actuelle des établissements.

Le rapport ne préconise pas une refonte globale du secret bancaire français, et encore moins sa suppression. Il n'entend pas plus priver les personnes de la confidentialité qui s'attache à leurs données et reste unanime quant à la nécessité de préserver cet élément essentiel de la relation bancaire, que ce soit par le biais du secret professionnel ou par l'usage de clauses ou d'accords de confidentialité assurant le même niveau de protection aux personnes, comme c'est le cas dans de nombreux pays.

À la lumière des différents constats développés dans le présent rapport, des évolutions ciblées au cadre légal actuel ont néanmoins été identifiées comme souhaitables. Il est ainsi proposé une clarification de certaines exceptions existantes, notamment dans le domaine des opérations de M&A bancaire et les transferts d'informations au sein des groupes bancaires. Il est également préconisé de créer de nouvelles exceptions en réponse aux difficultés opérationnelles que les établissements assujettis rencontrent dans le cadre de leur recours croissant à la sous-traitance ou pour respecter leurs obligations réglementaires. Dans la mesure où le présent rapport ne propose pas une refonte complète du secret bancaire, les évolutions ciblées qu'il recommande, essentiellement de nature technique, devraient faire l'objet d'interventions législatives progressives et ponctuelles.

Le présent rapport met également en lumière la coexistence complexe de l'obligation de secret bancaire avec certains régimes juridiques introduits par les réglementations européennes récentes (RGPD et DPS2). Cette complexité devrait amener les pouvoirs publics à une **réflexion sur la nécessaire modernisation des textes pour mieux articuler ces législations encadrant, d'une façon générale, les données et informations des personnes.**

Les évolutions proposés dans le rapport permettraient une **meilleure adéquation** de cette obligation au contexte et aux organisations actuelles **tout en préservant les objectifs du secret bancaire** : la protection des intérêts privés des clients ainsi que la sécurité et le bon fonctionnement du système bancaire français.

TABLE DES MATIÈRES

I- Objet et champ d'application du secret bancaire : rappel du droit positif

Le régime juridique et le champ d'application du secret bancaire sont légalement encadrés par les articles L.511-33 et L.522-19 du Code monétaire et financier. Les sanctions qui y sont attachées sont quant à elles prévues aux articles L.571-4 et L.572-7 du Code monétaire et financier qui renvoient aux dispositions de l'article 226-13 du Code pénal.

Après un rappel sur sa nature (1.1), les acteurs concernés (1.2) et l'information couverte par le secret (1.3), la présente section exposera les situations dans lesquelles le secret bancaire est partagé (1.4) et les exceptions prévues par la réglementation (1.5). Un rappel des sanctions sera également réalisé (1.6).

Il est également apparu opportun au groupe de travail d'intégrer une étude synthétique sur l'encadrement du secret bancaire au sein de plusieurs pays de l'Union européenne, de la Suisse et des États-Unis (1.7).

1.1 - La nature du secret bancaire

Le secret professionnel connaît en droit français deux natures :

- un secret professionnel « absolu », fondé exclusivement sur la protection de l'intérêt public, opposable à la justice et qui ne peut pas être levé par la personne qui en bénéficie. Il s'agit, notamment, du secret professionnel auquel les professions médicales sont astreintes ;

- un secret professionnel dit « relatif » comportant des exceptions et dont le professionnel assujetti peut être délié par la personne qui en bénéficie.

Le secret bancaire entre dans cette seconde catégorie. L'obligation à laquelle sont assujetties les banques connaît de nombreuses exceptions, en évolution constante au gré de la jurisprudence, et la personne protégée par le secret reste libre de délier l'établissement assujetti de son obligation (*cf. infra – section I/ D/ et E/*).

La nature relative du secret bancaire et, en particulier, la possibilité pour la personne protégée d'y renoncer, tiennent en priorité à la préservation d'un intérêt privé[8].

[8] *J. LASSERRE CAPDEVILLE, Le secret bancaire, Étude de droit comparé (France - Suisse – Luxembourg), Presses Universitaires d'Aix-Marseille (2006), n° 210 et suivants.*

Dans ses relations avec son client, l'établissement assujetti est amené à connaître non seulement des informations d'ordre financier et patrimonial le concernant, mais également des informations d'ordre personnel. Le banquier tenant, *de facto*, un rôle de « *confident nécessaire* », le secret devient un élément essentiel de cette relation[9]. La sauvegarde de l'intérêt privé de son client fonde, par voie de conséquence et en premier lieu, l'obligation de discrétion à laquelle l'établissement est tenu à son égard.

Si la doctrine s'accorde sur le caractère prédominant de cet objet d'ordre privé, la préservation d'un intérêt public demeure également un des fondements du secret bancaire[10]. L'institution d'un secret pesant sur les informations dont les établissements assujettis disposent dans l'exercice de leurs activités est un élément essentiel au bon fonctionnement du système bancaire et, plus généralement, à la sécurité des affaires, qui doivent, tous deux, reposer sur un système de confiance réciproque.

1.2 - Les acteurs du secret bancaire

1.2.1 - Les personnes tenues au secret bancaire

D'une façon générale, le secret bancaire s'impose, en vertu des articles L.511-33 et L.522-19 du Code monétaire et financier, notamment aux établissements suivants[11] :

- les établissements de crédit[12] ;
- les sociétés de financement[13] ;
- les organismes mentionnés au 5[14] et 8[15] de l'article L.511-6 du Code monétaire et financier ;
- les établissements de paiement[16].

---

[9] *C. GAVALDA et J. STOUFFLET, Droit bancaire, Institutions comptes opérations services, Litec 6e édition, n°174 / S. PIEDELIEVRE et E. PUTMAN, Droit bancaire, Économica, n° 192.*

[10] *Justifiant, probablement et notamment, l'existence de la sanction pénale en cas de violation du secret bancaire.*

[11] *Les travaux du Groupe se sont concentrés sur le secret professionnel applicable, en vertu des articles L.511-33 et L.522-19 du Code monétaire et financier, aux établissements de crédit, aux sociétés de financement, aux organismes mentionnés aux 5 et 8 de l'article L.511-6 du Code monétaire et financier ainsi qu'aux établissements de paiement.*

Si les travaux n'ont en revanche pas spécifiquement porté sur le secret professionnel applicable aux prestataires de services d'investissement (Titre III du Livre V du Code monétaire et financier) régi par l'article L.531-12 du même code, les dispositions de cet article sont très proches de celles figurant aux articles L.511-33 et L.522-19, de telle sorte que les recommandations formulées au sein du rapport apparaissent, en grande partie, transposables au sein de l'article L531-12 du Code monétaire et financier.

[12] *Art. L511-1 I CMF.*

[13] *Art. L511-1 II CMF.*

[14] *« associations sans but lucratif et […] fondations reconnues d'utilité publique accordant sur ressources propres et sur ressources empruntées des prêts pour la création, le développement et la reprise d'entreprises dont l'effectif salarié ne dépasse pas un seuil fixé par décret ou pour la réalisation de projets d'insertion par des personnes physiques ».*

[15] *« sociétés de tiers-financement définies à l'article L. 381-2 du code de la construction et de l'habitation dont l'actionnariat est majoritairement formé par des collectivités territoriales ou qui sont rattachées à une collectivité territoriale de tutelle ».*

[16] *Art. L522-1 I CMF.*

De façon plus précise, ces deux articles listent les personnes qui, au sein de ces établissements, sont expressément tenus de respecter le secret et qui encourent la sanction prévue à l'article 226-13 du Code pénal en cas de violation du celui-ci. Il s'agit :

- des membres du conseil d'administration ou, le cas échéant, du conseil de surveillance ;
- de toute personne participant, à un titre quelconque, à la direction ou à la gestion de l'établissement ;
- de toute personne employée par l'établissement (en ce compris les stagiaires, alternants, etc.), quelle que soit leur affectation (siège, agences, filiales, succursales, bureaux de représentation) ou leur position dans la hiérarchie, et peu importe qu'elle soit ou non en contact avec la clientèle de l'établissement.

À cette liste s'ajoutent également, conformément aux dispositions des articles L.511-33 I alinéa 6 et L.522-19 I alinéa 5 du Code monétaire et financier, toutes les personnes qui, à l'occasion de leur fonction, obtiennent communication d'informations couvertes par le secret[17] ainsi que toutes les personnes qui participent aux missions de contrôles confiées à l'Autorité de Contrôle Prudentiel et de Résolution (ACPR)[18] et la Banque Centrale Européenne (BCE).

1.2.2 - Les personnes couvertes par le secret bancaire

Contrairement aux personnes devant respecter le secret, la loi ne précise pas les personnes qui en bénéficient.

Le secret bancaire ayant été édicté dans l'objectif de protéger l'ensemble des personnes, physiques ou morales, à propos desquelles l'établissement a obtenu des informations confidentielles (en sa qualité de « *confident nécessaire* » - cf. *supra – section I/ A/*), son champ d'application s'envisage, dès lors, largement.

Peu importe que les informations concernent un client de l'établissement ou toute autre personne : toute personne peut revendiquer la protection due au titre du secret bancaire dès lors qu'un établissement assujetti a eu connaissance, dans l'exercice de son activité, d'informations confidentielles concernant cette personne.

Le secret bancaire bénéficie, naturellement et dans la majorité des cas, aux personnes (physiques ou morales) clientes des établissements assujettis. Rappelons à ce titre que, de jurisprudence constante,

---

[17] *Ces dispositions disposent que ces personnes « doivent […] conserver [les informations] confidentielles » et qu'elles peuvent, à leur tour, communiquer ces informations dans les mêmes conditions que celles visées par ces mêmes articles.*

[18] *Art. L512-17 du Code monétaire et financier.*

l'obligation de confidentialité ne prend fin ni à la clôture de la relation contractuelle entre l'établissement et son client[19], ni au décès du titulaire du compte[20].

Compte tenu de la nature de leurs activités, les établissements assujettis recueillent également nombre d'informations sur des personnes avec lesquelles ils n'entretiennent aucune relation contractuelle. Il n'y a, aujourd'hui, aucun doute sur le fait que le bénéfice du secret doit également être accordé à ces « tiers ».

La jurisprudence l'a affirmé à de nombreuses reprises, à commencer par le bénéficiaire d'un chèque dont les informations sont contenues au sein des endos[21], mais également s'agissant du mandataire chargé de faire fonctionner le compte du client[22] et du garant de ses obligations[23]. Ainsi, les tiers, bénéficiaires ou donneurs d'ordres de tout type d'opérations de paiement passées sur le compte des clients (au débit ou au crédit) des établissements assujettis, bénéficient également de la protection du secret bancaire[24].

1.3 - L'information couverte par le secret bancaire

Les dispositions du Code monétaire et financier sont également muettes sur l'objet même du secret bancaire et se contentent d'évoquer, sans plus de précisions, « *les informations couvertes par le secret professionnel* ».

C'est la jurisprudence qui a apporté des clarifications sur la nature des informations couvertes par le secret ainsi que sur les critères permettant de faire entrer ces informations dans le champ d'application des dispositions légales. Elle a notamment précisé que :

- la violation du secret professionnel résulte de la divulgation par le dépositaire du secret de « *précisions qu'il était le seul à connaître* »[25] ;

[19] *Civ. 1er, 2 juin 1993, n° 90-21.982, Bull. civ. I, n° 397.*

[20] *Com. 9 juin 2004, n° 02-19.572, JurisData n° 2004-024182, JCP E 2004, n° 1739, obs. C. Caron.*

[21] *Voir encore récemment Com., 15 mai 2019, n° 18-10.491.*

[22] *Voir notamment Com., 25 févr. 2003, Bull. civ. IV, n° 26, p. 30 ; Banque et droit n 89, mai-juin 2003. 56, obs. Bonneau ; Rev. dr. bancaire et financier n° 2, mars-avril 2003. 92, obs. Crédot et Gérard ; D. 2003, act. jurisp. 1162, obs. Avena-Robardet ; Rev. trim. dr. com. 2003. 343, obs. Legeais ; JCP 2003, éd. G, 10195, note Ayissi Manga.*

[23] *Voir notamment TGI Nanterre, 6 ch., 25 mai 2010, Banque et droit n 133, sept.-oct. 2010. 37, obs. Bonneau.*

[24] *Et à ce titre, hors exceptions légales, seuls ces tiers peuvent donner mainlevée du secret à l'établissement teneur de compte sur ces informations (et non le titulaire dudit compte, client de l'établissement).*

[25] *Crim. 7 mars 1989, n° 87-90500, Bull. Crim. 1989 n° 109 p. 290.*

- « *l'obligation au secret professionnel à laquelle sont tenus les établissements de crédit leur interdit de fournir à un client qui en formule la demande des renseignements autres que simplement commerciaux d'ordre général et économique sur la solvabilité d'un autre de leurs clients* »[26] ; et que

- l'information est couverte par le secret professionnel uniquement si elle est reçue à titre professionnel[27].

Ainsi, pour bénéficier du secret, il est communément admis que les informations doivent répondre aux trois critères cumulatifs suivants :

(i) avoir été reçues dans l'exercice ou à l'occasion de son activité professionnelle : seules les informations reçues dans ce cadre sont susceptibles de protection, à l'exclusion de celles recueillies à titre personnel ;

(ii) avoir un caractère confidentiel : peu importe que l'information soit également connue d'autres personnes, l'établissement assujetti demeure tenu au secret ;

(iii) être suffisamment précises : l'information doit être de nature à porter atteinte, si elle était divulguée, au secret des affaires pour les entreprises ou au secret de la vie privée pour les personnes physiques.

En revanche, n'entrent pas dans le champ d'application du secret bancaire :

- les informations qui ont un caractère général et qui correspondent à l'opinion de la place, appelées « *renseignements commerciaux* »[28] ;

- les informations qui sont du domaine public. Il en est ainsi de certaines informations qui peuvent être appréhendées par toute personne auprès d'un organisme extérieur officiel tel qu'un greffe (par ex. l'extrait RCS, le bilan d'une société tenue de le déclarer, etc.). Soulignons toutefois que des informations révélées par la presse demeurent couvertes par le secret.

Ainsi, et à titre d'exemples, la jurisprudence a pu admettre que répondent aux critères de confidentialité et de précision :

- l'existence même d'un compte et sa nature, l'existence d'une donation, d'assurances, etc. et, *a fortiori*, l'identité des titulaires d'un compte, d'un placement, l'identité d'un emprunteur, mais également des mandataires, des cautions, etc. ;

---

[26] *Com. 18 mars 2007, n° 06-10663, Bull. 2007, IV, n° 195.*

[27] *Civ., 3 nov. 2004, n° 02-19211.*

[28] *J-L. RIVES-LANGE, M. CONTAMINE-RAYNAUD, Droit bancaire, Précis Dalloz 6e édition, n° 177.*

- le solde d'un compte, le détail des écritures, le montant de certaines opérations (crédits, mouvements, prestations sociales, etc.), les versements périodiques faits par un client à une tierce personne (en ce compris l'identité de ce tiers) et, plus généralement, le relevé de compte ;

- les informations relatives à l'épargne (au sens large) détenues par un client (titres, placements, etc.), la location d'un compartiment de coffre-fort, l'achat de bons d'épargne, d'or, etc. ;

- les opérations de caisse ou de portefeuille (versement de sommes d'argent, paiement de chèques), les opérations sur titres ;

- la notation / *scoring* d'un client réalisé par un établissement[29] ;

- les incidents de paiement, les interdictions d'émettre des chèques, les demandes de report d'échéances, les rejets de chèques, etc. ;

- les règlements amiables avec ou sans ouverture de procédure collective ;

- l'octroi ou le refus de crédit, l'existence d'un découvert, la souscription de garanties au profit de la banque ;

- le contenu d'un document comptable communiqué par le client (sauf lorsque ce document est publié au greffe et fait donc partie du domaine public) ;

- la composition des organes dirigeants, accords ou ententes avec d'autres entreprises ;

- l'existence de brevets ;

- tous projets et tous actes, protocoles, conventions, documents contractuels.

1.4 - Le secret partagé

Le secret bancaire étant relatif, celui-ci peut être partagé avec certaines personnes qui peuvent faire valoir les mêmes droits que le créancier initial du secret, ou qui se sont vues confier, par ce dernier, la gestion de ses affaires ou encore qui agissent de droit ou sur ordre de l'autorité judiciaire dans l'intérêt du client.

---

[28] *J-L. RIVES-LANGE, M. CONTAMINE-RAYNAUD, Droit bancaire, Précis Dalloz 6e édition, n° 177.*

[29] *Certains auteurs considèrent que « L'élaboration d'un score, essentiellement pour mesurer la qualité financière d'un client, passe par une approche multicritères dont la synthèse est un élément qualitatif qui, sans être très précis, n'en constitue pas moins une redoutable source d'informations. On doit pouvoir considérer que le score, qui reflète généralement une situation financière, doit être protégé par le secret au même titre que les éléments qui ont conduit à sa détermination. » (D. Valette et C. Lassalas, Le secret bancaire au sein des groupes non bancaires, Revue Lamy droit des affaires n° 53, 1er octobre 2002).*

1.4.1 - La révélation consentie par la personne protégée

(i) Le Code monétaire et financier[30] a intégré en 2008 la possibilité pour les personnes de délier l'établissement assujetti de son obligation au secret vis-à-vis des tiers non couverts par l'une des exceptions prévues par la réglementation (cf. *infra*).

Notons que si la profession bancaire s'est félicitée de cette codification, la loi de modernisation de l'économie en a néanmoins resserré significativement les contours et les conditions de validité.

D'une part, les articles L.511-33 et L.522-19 du Code monétaire et financier imposent un consentement exprès là où la jurisprudence antérieure admettait que la mainlevée puisse être donnée tacitement par l'intéressé[31].

D'autre part, l'autorisation doit être donnée préalablement par la personne, imposant ainsi aux établissements de prévoir des clauses dites « de levée du secret bancaire » les plus précises et claires possible, tant sur la portée de l'engagement de la personne, que sur les informations pour lesquelles la personne protégée renonce au secret ou sur les opérations pour lesquelles le secret est levé.

Notons qu'en pratique, ces clauses sont insérées dans les conventions d'ouverture de compte dans le respect de ces principes[32]. Ces clauses font, à ce titre, régulièrement l'objet de modifications pour s'adapter aux évolutions d'organisation ou aux nouveaux projets des établissements assujettis par application de la procédure de l'article L.312-1-1 du Code monétaire et financier qui organise un dispositif légal d'obtention du consentement du client.

(ii) Le secret bancaire peut être partagé avec le mandataire conventionnel choisi par le client. Il convient de préciser que ce mandataire n'aura accès au secret que dans la limite de son mandat. Le secret doit en revanche lui être opposé pour tout ce qui est étranger à sa mission[33] ou s'agissant de toutes informations ou confidences personnelles intéressant ou émanant du mandant ou encore des affaires particulières dans lesquelles le banquier est intervenu ou dont il a eu connaissance.

---

[30] *Article L.511-33 I, 12e alinéa et L.522-19 I, 9e alinéa du Code monétaire et financier.*

[31] *Com. 11 avril 1995, n° 92-20.985, Bull. civ. IV, n° 121.*

[32] *Deux décisions ont sanctionné des clauses contraires à ces principes : l'une ayant affirmé l'impossibilité de prévoir une clause générale de levée du secret bancaire dans un contrat (Com. 11 avril 1995, n° 92-20.985), l'autre ayant jugé abusive pour ces motifs une clause de levée du secret bancaire incluse dans une convention d'ouverture d'un compte de dépôt (CA Douai, 27 février 2008, 1re chambre, 2e section, n° 06/07192).*

[33] *À titre d'exemple, une procuration octroyée pour faire fonctionner un compte autorisera le banquier à fournir au mandataire, à sa demande, des relevés d'opérations ou des relevés de compte. Le droit pour le mandataire à partager le secret pour ce qui ressort de sa mission ne s'étend néanmoins pas aux opérations ordonnées par le client avant qu'il ait donné procuration, ni à celles effectuées postérieurement à la révocation (ou à la renonciation) du pouvoir.*

(iii) Le secret peut également être partagé dans le cadre de comptes comportant plusieurs titulaires. Ayant accepté de « *partager* » le compte avec une ou plusieurs autres personnes, le client accepte, *de facto*, le partage du secret concernant ce compte avec les co-titulaires. Il convient néanmoins de préciser que le secret bancaire ne peut être opposé aux autres co-titulaires que dans les limites suivantes : le partage doit être limité aux écritures du compte et à la communication des pièces y afférentes et l'information ne s'étend pas, en principe, aux faits et actes intéressant une seule des parties.

(iv) Citons, enfin, le secret partagé dans le cadre des dispositifs de médiation offerts aux clients des banques qui, en saisissant le médiateur compétent, acceptent *de facto* la communication par l'établissement à ce dernier d'informations couvertes par le secret bancaire[34].

1.4.2 - Les intervenants sur le compte des clients protégés ou incapables

(i) Le secret bancaire ne peut être opposé au(x) représentant(s) légal(aux) du mineur. *A fortiori*, au sein de familles biparentales, l'un ou l'autre parent peut avoir accès aux informations concernant les opérations bancaires du mineur, qu'elles soient effectuées par l'un ou l'autre des parents ou par le mineur seul.

Par ailleurs, lorsque le mineur est placé sous tutelle, le tuteur a accès à l'information sur les opérations effectuées par le mineur. Pour l'exercice de sa mission, le subrogé tuteur doit pouvoir accéder aux comptes du mineur.

Le juge des tutelles peut également y avoir accès, le cas échéant par l'intermédiaire du directeur des services de greffe judiciaires[35], en particulier lorsqu'il n'obtient pas les informations prévues des administrateurs légaux ou du tuteur. En revanche, vis-à-vis du conseil de famille, le secret doit être maintenu sauf accord exprès du tuteur ou décision du juge des tutelles.

En tout état de cause, le droit du représentant légal (parent ou tuteur) cesse à la majorité ou lors de l'émancipation de l'enfant.

---

[34] S'agissant du Médiateur du crédit aux entreprises, l'article 17 de l'accord de place (disponible ici) conclu entre l'État, la Banque de France, les instituts d'émission en Outre-mer, la Fédération Bancaire Française (FBF) et l'Association française des sociétés financières (ASF) précise que « la saisine de la Médiation induit en effet l'autorisation [de l'entreprise à l'initiative de la saisine] de lui communiquer des éléments confidentiels relatifs à l'entreprise l'ayant saisie et délie ainsi les collaborateurs des établissements vis-à-vis du médiateur du crédit de leur obligation de secret. À cet effet, une mention appropriée figure dans le formulaire de saisine du dossier de Médiation ». S'agissant de la médiation des litiges de la consommation (dont le régime est fixé aux articles L.611-1 et suivants du Code de la consommation et applicable au secteur financier conformément à l'article L.316-1 du Code monétaire et financier), ce même principe de levée du secret par le client à l'initiative de la saisine est, en règle générale, rappelé dans les chartes ad'hoc adoptées par les Médiateurs désignés.

[35] Cf. article 387-5 du code civil.

(ii) S'agissant des majeurs placés sous un régime de protection et en particulier des majeurs sous tutelle, il convient de retenir que le secret bancaire n'est pas opposable au tuteur qui représente le majeur protégé dans les actes nécessaires à la gestion de son patrimoine. En revanche, la doctrine considère que « *l'incapacité d'exercice qui touche la personne protégée donnerait à l'établissement de crédit le droit d'opposer le secret bancaire à son propre client* »[36], privant notamment le majeur placé sous une mesure de tutelle d'un droit de regard sur son compte.

Par ailleurs, bien qu'aucun texte ne prévoie de levée générale du secret bancaire au bénéfice du curateur, dès lors que, comme le tuteur, le curateur, dans le cadre d'une curatelle renforcée, dispose « *d'un pouvoir de gestion, souvent exclusif, sur tous les comptes personnels du majeur protégé* », la doctrine considère qu'il doit pouvoir bénéficier d'une « *levée du secret bancaire à l'égard des informations nécessaires à l'exercice de sa mission* »[37].

En matière de curatelle simple, le majeur protégé peut accomplir seul les actes conservatoires et les actes d'administration. *A contrario*, l'assistance de son curateur est requise pour l'accomplissement d'actes de disposition[38]. Le curateur étant tenu de « r*endre compte au juge du bon exercice de sa mission* », le secret bancaire ne doit pas lui être opposé[39]. Toutefois, une partie de la doctrine considère que le secret bancaire n'est inopposable au curateur que dans la limite des pouvoirs qui lui ont été accordés par le juge[40].

Les majeurs sous sauvegarde de justice conservent l'exercice de leurs droits[41]. Dans la mesure où ils sont capables et non juridiquement représentés, ils ont seuls le droit à l'information. Néanmoins, le juge peut désigner un mandataire spécial à l'effet d'accomplir un ou plusieurs actes déterminés. Dans ce cas, l'alinéa 2 de l'article 510 du Code civil, auquel renvoie l'article 437 du même code, prévoit un droit de communication dans le cadre duquel le secret bancaire ne peut pas être opposé, afin que le mandataire spécial puisse rendre compte de son mandat.

Concernant le mandat de protection future, le mandataire représente le client de la banque dans le cas où il ne peut plus pourvoir seul à ses intérêts[42]. Aussi, la banque ne peut lui opposer le secret bancaire s'agissant des informations qui entrent dans le cadre de son mandat.

---

[36] G. RAOUL-CORMEIL et J. LASSERRE CAPDEVILLE, Le droit de regard sur les comptes d'un majeur protégé, Revue de droit bancaire et financier n° 3, Mai 2013, 26.

[37] G. RAOUL-CORNEIL et J. LASSERRE CAPDEVILLE, Le droit de regard sur les comptes d'un majeur protégé, ibid.

[38] Article 467 du Code civil.

[39] G. RAOUL-CORNEIL et J. LASSERRE CAPDEVILLE, Le droit de regard sur les comptes d'un majeur protégé, ibid.

[40] En ce sens : F. BORDAS, Fascicule 141 : Devoirs professionnels des établissements de crédit – Secret bancaire, JurisClasseur Banque – Crédit – Bourse, 11 juin 2015 (dernière mise à jour : 27 septembre 2016).

[41] Article 435 du Code civil.

[42] Article 477 du Code civil.

Enfin, pour ce qui est de l'habilitation familiale, la personne habilitée est fondée à obtenir la communication des informations relatives aux actes qu'elle a le pouvoir d'accomplir seule (habilitation familiale en représentation) ou pour lesquels une assistance du client protégé est nécessaire (habilitation familiale en assistance).

1.4.3 - Le secret partagé dans les rapports de famille

(i) Si, entre époux, le principe reste celui d'une opposabilité du secret bancaire sur les informations confidentielles de chacun d'eux, certaines exceptions existent.

Ainsi, l'époux peut accéder, exceptionnellement, à l'information protégée lorsqu'il bénéficie de la représentation judiciaire en vertu des articles 219[43] ou 1429, alinéa 1[er 44] du Code civil. Un époux peut également obtenir de la justice la levée du secret bancaire dans le cadre de mesures urgentes pouvant être prises en vertu de l'article 220-1 du Code civil (ex : blocage des comptes) ou accéder aux informations couvertes par le secret lorsqu'il est substitué à son conjoint défaillant en vertu de l'article 1426 du Code civil[45].

(ii) Dans le cadre d'une procédure de divorce judiciaire ou de séparation de corps en cours, le juge aux affaires familiales peut ordonner la communication de renseignements relatifs aux avoirs de l'un ou l'autre des époux sans que le secret bancaire ne puisse lui être opposé[46]. Cette règle constitue une exception au principe de non-communicabilité des informations bancaires aux juges civils.

Par ailleurs, lors de la dissolution du régime matrimonial (divorce, séparation de corps ou de biens), le solde du compte bancaire peut faire partie de l'actif à partager. Aussi, si le conjoint du client peut faire valoir ses droits sur ce solde, le secret ne lui sera pas opposable. Notons également que, concernant le notaire, ce n'est que lorsque le divorce, la séparation de corps ou la séparation de biens ou le changement de régime matrimonial, sera prononcé par décision de justice devenue définitive que la banque pourra, sans autorisation préalable du titulaire du compte, communiquer au notaire

---

[43] « Si l'un des époux se trouve hors d'état de manifester sa volonté, l'autre peut se faire habiliter par justice à le représenter, d'une manière générale, ou pour certains actes particuliers, dans l'exercice des pouvoirs résultant du régime matrimonial, les conditions et l'étendue de cette représentation étant fixées par le juge. […] ».

[44] Lorsque l'un des époux obtient du juge le pouvoir d'administrer les biens de l'autre époux, lorsque ce dernier « se trouve, d'une manière durable, hors d'état de manifester sa volonté, ou s'il met en péril les intérêts de la famille ».

[45] « Si l'un des époux se trouve, d'une manière durable, hors d'état de manifester sa volonté, ou si sa gestion de la communauté atteste l'inaptitude ou la fraude, l'autre conjoint peut demander en justice à lui être substitué dans l'exercice de ses pouvoirs […]. Le conjoint, ainsi habilité par justice, a les mêmes pouvoirs qu'aurait eus l'époux qu'il remplace ; il passe avec l'autorisation de justice les actes pour lesquels son consentement aurait été requis s'il n'y avait pas eu substitution. […] ».

[46] Article 259-3 du Code civil.

se référant à la décision judiciaire (jugement de divorce ou d'homologation du changement de régime matrimonial) l'état des avoirs de celui-ci au jour de l'assignation, sauf disposition du jugement faisant remonter ses effets à la date à laquelle la collaboration et la cohabitation des époux ont cessé.

(iii) Le partage du secret bancaire existe enfin en matière de succession au profit des héritiers et légataires universels (sauf volonté contraire du défunt). Au regard du principe de continuité de la personne du défunt posé par le Code civil, le droit à l'information des héritiers et légataires universels est étendu non seulement au(x) compte(s) du défunt (les opérations effectuées du vivant du client décédé peuvent donc être communiquées aux héritiers) mais également aux documents d'ordre patrimonial que peut détenir le banquier concernant ce dernier.

Précisons néanmoins que le secret bancaire n'est pas levé s'agissant des faits de caractère purement personnel dont le banquier a pu avoir connaissance : l'accès aux informations ne s'étend pas aux informations concernant la vie privée du *de cujus* (par exemple le banquier n'a pas qualité pour révéler l'existence d'un enfant naturel). Il est par ailleurs bien évident que les héritiers et légataires universels ne sauraient avoir plus de droit que la personne du défunt qu'ils continuent. Aussi, n'ont-ils pas à en savoir plus que le défunt lui-même[47].

1.4.4 - Les organes des personnes morales et les commissaires aux comptes

(i) S'agissant des personnes morales, créancières du secret bancaire, le partage du secret bancaire existe, en principe et uniquement[48], au profit des représentants légaux qui peuvent, dès lors, accéder à tous les renseignements détenus par l'établissement assujetti sur l'entreprise qu'ils dirigent. C'est notamment le cas du gérant de sociétés commerciales ou civiles[49] ou du Président du Conseil d'administration d'une Société Anonyme[50].

En revanche, il convient de retenir qu'un administrateur, un membre du directoire (autres que ceux ayant la qualité de président du directoire ou de directeur général) ou un membre du conseil de surveillance n'aura pas accès aux informations confidentielles détenues par le banquier lorsqu'il agit personnellement et individuellement au nom ou pour le compte de la société sans être dûment mandaté (par le conseil d'administration, par exemple pour une société anonyme).

---

[47] En ce sens, cf. Pau, 15 mai 2006 et Com., 30 mai 2007, n° 06-11.036, à propos de bons anonymes.

[48] Les associés et/ou actionnaires doivent, dans tous les cas, se voir opposer le secret bancaire.

[49] Notamment pour le gérant de société commerciale ou de société civile : Com., 16 janvier 2001, n° 98-11.744, Bull. civ. IV, n° 12, D. 2001, AJ 545, obs. A. Lienhard.

[50] Voir en ce sens Th. BONNEAU, Président dissocié et secret bancaire. Des implications possible de la NRE, Dr. Sociétés, janv. 2002, n° 1.

(ii) Conformément aux deux derniers alinéas de l'article L.823-14 du Code de commerce, les banques, en leur qualité de tiers, peuvent être sollicitées par les commissaires aux comptes des S.A., SARL, SNC, SCS mais également des GIE et des personnes morales de droit privé non commerçantes (sociétés civiles, associations) quel que soit le moment de la vie de la société dont ils ont la charge (période de prospérité comme période de difficultés). Le secret bancaire est donc levé sur les seuls renseignements utiles à leur mission et liés à l'exploitation de la société.

1.4.5 - Les cautions

Pour terminer sur le secret partagé, il convient de rappeler que si le secret bancaire est, en principe, opposable à la caution s'agissant des informations relatives à la personne dont elle garantit les engagements auprès d'un établissement de crédit, ce principe connaît néanmoins des exceptions légales dans le cadre des informations obligatoires, ponctuelles ou régulières, que les établissements doivent communiquer à ladite caution[51].

1.5 - Les exceptions au secret bancaire

Nota : la présente section a pour objectif d'identifier les entités auxquelles le secret bancaire est inopposable en vertu d'un texte législatif ou réglementaire. Ces exceptions ne sont toutefois pas toutes générales : leurs modalités d'application et leurs limites ne sont pas détaillées dans le présent rapport et il convient de se référer aux textes et/ou à la jurisprudence pour en connaître précisément les contours.

1.5.1 - Les exceptions des articles L.511-33 et L.522-19 du Code monétaire et financier

Les articles encadrant le secret bancaire prévoient une liste limitative d'entités à qui le secret est inopposable :

(i) L'Autorité de contrôle prudentiel et de résolution (ACPR) : l'établissement assujetti doit répondre à toutes les demandes de l'ACPR entrant dans le domaine de compétences de cette dernière.

[51] *Il s'agit : (i) de l'information annuelle prévue par l'article L.313-22 du Code monétaire et financier de la caution qui garantit « un concours financier à une entreprise » ; (ii) de l'information ponctuelle prévue par l'article L.314-17 du Code de la consommation à destination de toute personne physique qui s'est portée caution de la défaillance du débiteur dès le premier incident caractérisé de paiement susceptible d'une inscription au fichier des incidents de remboursement des crédits aux particuliers (FICP) ; (iii) de l'information annuelle due aux cautions indéfinies prévue à l'article 2293 du Code civil ; (iv) des informations de la caution prévues aux articles L333-1 et L333-2 du Code de consommation.*

(ii) La Banque de France qui est « *est habilitée à se faire communiquer par les établissements bancaires et financiers tous documents et renseignements qui lui sont nécessaires pour exercer ses fonctions* »[52]. Notons par ailleurs que les établissements sont également tenus de réaliser de nombreuses déclarations (ponctuelles ou régulières) auprès des services de la Banque de France qui constituent autant d'exceptions au secret bancaire (auprès du service central des risques, dans le cadre des fichiers centraux en matière d'incidents sur chèques et effets – FCC, FIBEN, FICP, etc.).

(iii) Les établissements assujettis ne peuvent opposer le secret bancaire à l'**autorité judiciaire agissant dans le cadre d'une procédure pénale ou du prononcé des peines**[53]. Les établissements assujettis ne peuvent donc refuser ni de témoigner, ni de renseigner, ni de fournir les documents qu'ils détiennent sur le fondement du secret bancaire dans ce cadre.

Notons que le secret bancaire n'est levé qu'en considération de la qualité de la personne initiant la procédure pénale et du contexte dans lequel elle agit : le Procureur de la République, le juge d'instruction, les Officiers de Police Judiciaire (OPJ) agissant dans le cadre d'une procédure pénale[54], des Agents de Police Judiciaire agissant dans le même cadre que les OPJ sous le contrôle desquels ils agissent.

(iv) Les commissions d'enquête parlementaires créées en application de l'article 6 de l'ordonnance n° 58-1100 du 17 novembre 1958 relative aux fonctionnements des assemblées parlementaires modifiée par la loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires[55].

(v) Les agences de notation[56], uniquement pour les besoins de la notation des produits financiers.

(vi) Les personnes avec lesquelles l'établissement de crédit négocie, conclut ou exécute :

a. des opérations de crédit effectuées directement ou indirectement par un ou plusieurs établissements de crédit[57] ;

---

[52] *Article 5 de la loi du 3 janvier 1973 sur la Banque de France.*

[53] *Articles 60-1 et 99-3 du Code de procédure pénale et article 132-22 du Code pénal. Il convient de noter qu'il existe également d'autres cas de levée du secret bancaire à l'égard de l'agence de gestion et de recouvrement des avoirs saisis et confisqué (AGRASC) et de la plateforme interministérielle d'identification des avoirs criminels (PIAC) en vertu de l'article 695-9-51 du Code de procédure pénale.*

[54] *Dans le cadre d'une enquête de flagrance (article 53 du Code de procédure pénale) ou agissant sur instructions du Procureur de la République dans le cadre d'une enquête préliminaire (article 75 du Code de procédure pénale).*

[55] *L'article prévoit désormais notamment que : « Toute personne […] mentionnée au premier alinéa du I de l'article L. 511-33 du Code monétaire et financier est déliée du secret professionnel à l'égard de la commission, lorsque celle-ci a décidé l'application du secret […]. Dans ce cas, le rapport publié à la fin des travaux de la commission, ni aucun autre document public, ne pourra faire état des informations recueillies par levée du secret professionnel. ».*

[56] *Les agences de notation sont régies par le Règlement (CE) n° 1060/2009 du 16 septembre 2009 sur les agences de notation de crédit, tel que modifié par le Règlement (UE) n° 513/2011 du Parlement européen et du Conseil du 11 mai 2011.*

b. des opérations sur instruments financiers, de garanties ou d'assurance destinées à la couverture d'un risque de crédit ;

c. des prises de participation ou de contrôle dans un établissement de crédit, de paiement, une entreprise d'investissement ou une société de financement ;

d. des cessions d'actifs ou de fonds de commerce ;

e. des cessions ou transferts de créances ou de contrat ;

Cette exemption vise les titrisations, les transferts de participation dans les crédits syndiqués, les hypothèses où le recouvrement d'une créance a été confié à un tiers, ou lorsque la créance résultant d'une opération de crédit est cédée ou transférée à un tiers.

Par prudence, la doctrine[58] considère toutefois qu'il convient de ne pas transmettre aux investisseurs, par exemple dans le cadre de *Collateral Loan Obligation (CLO), « des informations précises concernant les prêts et leurs emprunteurs (telles que l'identité de l'emprunteur, le montant du prêt, les conditions financières et de remboursement, les sûretés éventuellement apportées, le score de crédit, etc.)* » par le biais du prospectus d'émission de titres ou tout autre document adressé aux investisseurs, dès lors que les emprunteurs n'ont pas expressément consenti à la levée du secret bancaire pour ce cas-là.

f. des contrat de prestations de services conclus avec un tiers en vue de lui confier des fonctions opérationnelles importantes[59] ;

g. lors de l'étude ou l'élaboration de tout type de contrats ou d'opérations, dès lors que ces entités appartiennent au même groupe.

Il convient de préciser que les bénéficiaires de la divulgation doivent garder confidentielles les informations divulguées, que l'opération aboutisse ou non. Lorsque l'opération aboutit, l'article L. 511-33 du Code monétaire et financier précise que ces bénéficiaires peuvent à leur tour communiquer les informations couvertes par le secret professionnel dans les mêmes conditions que celles visées

---

[57] Cette dérogation vise notamment les opérations de « pools bancaires ». Elle permet également de faire exception au secret dans le cadre de la transmission des informations nécessaires à la mise en place de cautionnements délivrés par des organismes spécialisés en garantie de crédits, notamment immobiliers.

[58] F. LACROIX, Réforme du secret bancaire : vers une sécurité accrue des contrats de crédit, Revue Banque, n° 706, oct. 2008, p. 54 et s.

[59] Notons à propos de cette exception un arrêt de la Cour d'appel de Monaco (CA corr., Monaco, 30 mai 2011, Mme Y., PG n° 2006/001724) selon lequel « un établissement de crédit monégasque, auquel l'art. L. 511-33 est applicable, ne viole pas le secret bancaire en transmettant des informations de nature confidentielle à une société avec laquelle il a conclu un contrat afin de bénéficier d'une assistance juridique, dans la mesure où cette communication est indispensable pour qu'un conseil pertinent puisse être délivré » (Code monétaire et financier - Dalloz, Note 25 sous l'article L. 511-33).

à l'article L.511-33 aux personnes avec lesquelles ils négocient, concluent ou exécutent les opérations concernées.

Outre ces exceptions listées par les articles L.511-33 et L.522-19 du Code monétaire et financier, il convient de noter que l'article L.511-34 du Code monétaire et financier prévoit également des exceptions au secret bancaire afin de permettre aux entités d'un groupe financier de s'échanger certaines informations. Les informations devant être échangées au sein d'un groupe concernent les informations nécessaires (i) à la surveillance sur base consolidée, (ii) au dispositif de LCB-FT, (iii) à la détection des abus de marché et (iv) à la gestion des conflits d'intérêts.

Cette exception est strictement limitée au groupe et les informations ci-dessus « *ne peuvent être communiquées à des personnes extérieures au groupe, à l'exception des autorités compétentes* » des États membres de l'Union européenne, des États parties à l'accord sur l'Espace économique européen ou dans les États où l'ACPR ou l'AMF ont conclu des accords avec les autorités homologues. Toutefois, le secret bancaire reste applicable à l'égard des « *autorités des États ou territoires dont la législation est reconnue insuffisante ou dont les pratiques sont considérées comme faisant obstacle à la lutte contre le blanchiment des capitaux ou le financement du terrorisme par l'instance internationale de concertation et de coordination en matière de lutte contre le blanchiment d'argent* ».

Les personnes qui reçoivent les informations ci-dessus sont également tenues au secret professionnel conformément à l'article L.511-33 du Code monétaire et financier.

1.5.2 - Les exceptions créées par des lois spécifiques : autorités publiques au profit desquelles le secret bancaire est levé

(i) L'Administration fiscale à laquelle les établissements de crédit sont tenus de faire des déclarations[60], de communiquer certains documents en vertu de son droit de communication[61] ou dans le cas de procédures d'investigations menées par elle[62]. Notons également la levée du secret bancaire dans le cadre de l'application du *Foreign Account Tax Compliance Act* (FATCA)[63].

[60] *Déclaration des ouvertures et fermetures de comptes (Art. 1649 A du Code général des impôts), déclaration récapitulative annuelle des opérations sur valeurs mobilières et des revenus des capitaux mobiliers de leurs clients (Art. 242 ter 1 du Code général des impôts), déclaration des avoirs des clients décédés (Art. 806 du Code général des impôts), déclaration à la demande relatif aux comptes collectifs avec solidarité aux décès d'un déposant (Art. 808 du Code général des impôts), communication, sur sa demande, de l'identité des personnes auxquelles ont été délivrées des formules de chèques non barrées (Art. L.96 du Livre des procédures fiscales et article L.131-71, alinéa 3 du Code monétaire et financier).*

[61] *Articles L.81, L.83 et L.85 du Livre des procédures fiscales. Étant précisé que ce droit de communication ne peut cependant être utilisé par le fisc que pour une affaire déterminée et non en général.*

[62] *En contrôle des transferts à l'étranger (Art. L.96 A du Livre des procédures fiscales), dans le cadre de procédures spéciales de visite et de saisie (Art. L.16 B du Livre des procédures fiscales).*

[63] *Par application du dispositif national mis en place par le biais de l'article 1649 AC du Code général des impôts dont le I.*

(ii) L'Administration des douanes peut obtenir des banques communication de divers documents en se fondant pour l'essentiel sur les articles 65 et 455 du Code des douanes.

(iii) L'Autorité des marchés financiers (AMF) qui, aux termes de l'article L.621-8-4 du Code monétaire et financier, peut se faire communiquer tous documents ou informations, quel qu'en soit le support, utiles à l'exercice de sa mission de veille et de surveillance.

(iv) La Banque centrale européenne (BCE) qui, dans le cadre du mécanisme de surveillance unique (MSU), dispose du pouvoir de demander des informations, de réaliser des enquêtes générales et de procéder à des inspections sur place. Ces pouvoirs sont énoncés aux articles 10 à 12 du Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la BCE des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit.

(v) La société de gestion du fonds de garantie de l'accession sociale à la propriété (SGFGAS) qui contrôle le respect de l'ensemble de la réglementation relative aux prêts conventionnés et procède à la diffusion du taux de référence applicable à ces prêts ainsi qu'à la collecte des informations statistiques sur la distribution de ces crédits par les établissements affiliés. La levée du secret bancaire est prévue aux termes de l'article L.315-5-1 du Code de la construction et de l'habitation qui prévoit que la SGFGAS est en charge du suivi réglementaire et statistique de ces opérations, ainsi que du contrôle, sur pièce ou sur place, de ces opérations. Elle se retrouve également au sein de la convention-type annexée à l'arrêté du 14 août 2000 modifiant l'arrêté du 22 novembre 1977 fixant les conditions dans lesquelles des banques ou établissements peuvent être habilités à consentir des prêts conventionnés et qui décrit les modalités des contrôles de la SGFGAS.

(vi) La Cour des comptes et les institutions associées. En vertu des articles L141-5 du Code des juridictions financières, la Cour de comptes est habilitée à accéder à tous documents, données et traitements, de quelque nature que ce soit, relatifs à la gestion des services et organismes soumis à son contrôle ou nécessaires à l'exercice de ses attributions, et à se les faire communiquer. L'article L.141-9, I du Code des juridictions financières précise en outre que : « *Les agents des services financiers sont déliés du secret professionnel à l'égard des membres et personnels de la Cour des comptes mentionnés aux sections 1 à 5 du chapitre II du titre Ier du présent livre [magistrats, conseillers maîtres en service extraordinaire, etc.], à l'occasion des contrôles que ceux-ci effectuent dans le cadre de leurs attributions. Pour les besoins des mêmes contrôles, les membres et personnels de la Cour des comptes mentionnés aux mêmes sections 1 à 5 peuvent exercer directement le droit de communication que les agents des services financiers tiennent de la loi.* ».

Face aux difficultés d'interprétations de ces dispositions (en particulier des termes « *agents des services financiers* »), le Directeur du Trésor a dû prendre position dans une lettre du 24 juillet 1992. Interrogé par le Procureur Général près la Cour des comptes sur les modalités d'exercice du droit de communication des magistrats de la Cour des comptes spécifiquement auprès des établissements de crédit, le Directeur du Trésor ne donne pas de définition de la notion de « *services financiers* » mais

a rappelé que « *s'agissant des agents des services fiscaux* » (qu'il englobe donc dans la notion mais n'assimile pas), le droit de communication s'exerce vis-à-vis des établissements de crédit, sur le fondement des articles L.83 et L.85 du Livre des procédures fiscales. Il énonce les grands principes du droit de communication du fisc et conclut que même si les procédures suivant lesquelles s'exerce le droit de communication des administrations fiscales ne peuvent être transposées telles quelles au droit de communication direct des magistrats de la Cour des comptes, il lui paraît souhaitable qu'il s'exerce, vis-à-vis des établissements de crédit, dans des limites comparables. Il est ainsi favorable à ce que les magistrats de la Cour des comptes puissent demander aux établissements de crédit communication de relevés individuels de comptes d'un particulier ou d'une entreprise, de copies de chèques et de pièces annexes.

Suite à ce courrier, M. RAYNAUD, Procureur Général près la Cour des comptes, dans une lettre du 4 novembre 1992 adressée à M. TRICHET, l'assurait d'une part que les demandes adressées par les magistrats de la Cour des comptes mentionneraient la nature de l'enquête pour les besoins de laquelle ces magistrats exercent le droit de communication et d'autre part, que les demandes de communication de documents de services seraient désormais effectuées par son intermédiaire. L'AFEC (désormais connu sous le nom d'AFECEI) a, par courrier du 27 novembre 1992, informé tous ses correspondants de ces prises de positions. L'AFB en a fait de même pour ses adhérents.

(vii) Certains Ministères, notamment dans le cadre des contrôles menés par l'Inspection Générale des Finances en matière de prêts bonifiés[64] ou par la Direction départementale des territoires[65]. Le Ministère de l'économie et des finances bénéficie également d'une dérogation aux termes de l'article L.562-12, alinéa 1er du Code monétaire et financier qui permet aux services de l'État, en charge de la mise en œuvre des mesures de gel des avoirs (en particulier, le Trésor), de vérifier l'identité des personnes concernées auprès des établissements de crédit avant la publication desdites mesures de gel. Les banques doivent aussi informer les services de l'État à propos des mouvements des comptes des personnes concernées par ces mesures afin que ces services puissent apprécier le moment le plus adapté pour prendre une mesure de gel.

(viii) L'Autorité de la Concurrence, dans le cadre de ses pouvoirs d'enquête, de saisie et de visite[66].

(ix) Les agents habilités et disposant des pouvoirs d'enquête listés aux articles L.511.1 et suivants du Code de la consommation[67] (les agents de la Direction générale de la consommation, de la

[64] *Articles L.512-52 et L.512-53 du Code monétaire et financier.*

[65] *En matière de prêts agricoles bonifiés, les établissements prêteurs sont relevées du secret bancaire en faveur des inspecteurs de la Direction départementale des territoires.*

[66] *Articles L.450-1 à 450-8 du Code de commerce.*

[67] *Le Code de la consommation énonce en son article L.512-8 que « Les agents habilités peuvent exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission. Ils peuvent les obtenir ou en prendre copie, par tout moyen et sur tout support, ou procéder à la saisie de ces documents en quelques mains qu'ils se trouvent.». De surcroît, l'article L.512-3 du même code prévoit explicitement que le secret professionnel ne puisse leur être opposé : « Le secret professionnel ne peut être opposé aux agents agissant dans le cadre des pouvoirs qui leur sont conférés par le présent livre ».*

concurrence et de la répression des fraudes – DGCCRF et de la DDPP[68], les agents de l'office national de la chasse et de la faune[69]) ainsi que les **agents de la Banque de France commissionnés par le ministre chargé de l'économie** ainsi que les fonctionnaires chargés de missions de protection économique des consommateurs habilités par arrêté du ministre chargé de l'économie.[70]

(x) La Commission Européenne notamment dans le cadre de ses pouvoirs d'investigations dans les affaires de concurrence intracommunautaires afin de déceler les infractions commises par les entreprises. Les établissements habilités à distribuer des prêts bonifiés doivent, toujours dans le cadre des compétences intracommunautaires de la Commission, se soumettre à ces contrôles[71].

(xi) La Commission Nationale de l'Informatique et des Libertés (CNIL) conformément aux dispositions de l'article 19 III de la Loi n° 78-17 du 6 janvier 1978 modifiée.

(xii) TRACFIN notamment dans le cadre des obligations de déclaration définies aux articles L.561-15 à L.561-22 du Code monétaire et financier qui imposent aux professionnels assujettis de déclarer à TRACFIN les sommes qu'ils soupçonnent d'avoir une origine illicite.

(xiii) Le Fonds de garantie des dépôts et de résolution (FGDR) aux termes de l'article L.312-15, I du Code monétaire et financier qui dispose que le secret bancaire ne lui est pas opposable dans le cadre de sa mission d'indemnisation.

(xiv) Le Défenseur des droits aux termes de l'alinéa 2 de l'article 203 de la loi organique n° 2011-333 du 29 mars 2011 relative au Défenseur des droits.

(xv) La Haute Autorité pour la transparence de la vie publique qui « *peut se faire communiquer, sur pièce, par les représentants d'intérêts, toute information ou tout document nécessaire à l'exercice de sa mission, sans que le secret professionnel puisse lui être opposé.* »[72]

---

[68] *Article L511-3 du Code de la consommation qui habilite les agents de la DGCCRF à rechercher et constater des infractions ou des manquements indiqués aux articles L.511-5 à L.511-7 du Code de la consommation et pouvant concerner les établissements de crédit.*

[69] *Article L.511-22 du Code de la consommation qui mentionne les agents de l'article L.172-1 II 2° du Code de l'environnement.*

[70] *Article L.317-1 du Code monétaire et financier : ces agents « sont habilités à procéder dans l'exercice de leurs fonctions à la recherche et à la constatation par procès-verbal des infractions aux dispositions des articles L.312-1-1, L.312-1-2, L.314-12, L.314-13 et L.315-6 à L.315-8 du Code monétaire et financier ».*

[71] *Règlement n°1/2003 du conseil, 16 décembre 2002 : articles 17 à 28.*

[72] *Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite « Sapin 2 », art. 25. Cette disposition semble peu opérante dans le secteur bancaire, la mission de cette autorité ne devant, en pratique, par l'amener à connaître d'informations ou de documents qui seraient couverts par le secret bancaire.*

1.6 - Les sanctions encourues

1.6.1 - Les sanctions civiles

La responsabilité civile de l'établissement assujetti est engagée lorsqu'il révèle une information confidentielle en violation du secret bancaire. La personne ayant subi un préjudice du fait de la révélation de l'information confidentielle peut ainsi mettre en jeu la responsabilité civile contractuelle ou extracontractuelle[73] de l'établissement assujetti et demander la réparation de son dommage par le biais de dommages-intérêts.

En outre, il convient de noter qu'un établissement assujetti qui aurait révélé une information confidentielle en violation du secret bancaire, pourrait également être en situation d'atteinte illicite au secret des affaires si ladite information confidentielle était, par ailleurs, considérée comme une information protégée au titre du secret des affaires[74]. L'établissement engagerait, dès lors, sa responsabilité civile sur le fondement de l'article L.152-1 du Code de commerce qui dispose que « *Toute atteinte au secret des affaires telle que prévue aux articles L. 151-4 à L. 151-6 engage la responsabilité civile de son auteur* »[75].

Rappelons à ce titre qu'aux termes de l'article L.151-5 du Code de commerce : « *L'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation* » et que les sanctions civiles encourues sont celles prévues aux articles L.152-3 à L. 152-7 du Code de commerce [76].

1.6.2 - Les sanctions pénales

Les articles L.571-4 et L.572-7 du Code monétaire et financier sanctionnent par les peines figurant à l'article 226-13 du Code pénal le fait, pour les personnes mentionnées aux article L.511-33 et

---

[73] *Puisque, à côté des clients des établissements assujettis, la protection du secret bancaire bénéfice également aux personnes qui n'entretiennent aucune relation contractuelle avec l'établissement (cf. supra).*

[74] *L'article L.151-1 du Code de commerce précise que ces dernières répondent aux critères suivants : « 1° Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ; 2° Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret. ».*

[75] *Article introduit par la loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.*

[76] *Dommages-intérêts, mesures proportionnées de nature à empêcher ou à faire cesser l'atteinte au secret des affaires, astreintes, mesures de publicité de la décision, les cas échéant des mesures provisoires et conservatoires, le cas échéant le versement d'une indemnité à la partie lésée.*

le secret professionnel. Selon l'article 226-13 du Code pénal, l'infraction est constituée par la révélation d'une information à caractère secret par toute personne l'ayant reçue du fait de son état, de sa profession, d'une fonction ou d'une mission, temporaire ou non.

Notons que l'infraction peut être commise aussi bien par des personnes physiques que des personnes morales :

(i) s'agissant des personnes physiques, le délit de violation du secret professionnel est puni jusqu'à un an d'emprisonnement et par une amende pouvant atteindre 15.000 €, ainsi que par des peines complémentaires prévues par l'article 226-31 du Code pénal (dont notamment l'interdiction professionnelle) ;

(ii) s'agissant des personnes morales, elles peuvent se voir infliger une amende pouvant s'élever jusqu'à 75 000 euros, ainsi qu'une ou plusieurs peines complémentaires visées par l'article 131-39 du Code pénal.

La révélation de l'information protégée tient lieu d'élément matériel de l'infraction, peu importe le moyen de divulgation utilisé. Elle peut consister en la divulgation orale ou non, directe ou indirecte, de l'information secrète à tout tiers à qui l'information secrète a été transmise, ce tiers fût-il lui-même tenu au secret professionnel.

Par ailleurs, la révélation d'une information secrète n'est pas répréhensible sans constat de l'existence concomitante de l'intention de commettre l'infraction. Cette intention réside dans la conscience de révéler une information secrète, quel que soit le mobile qui a pu la déterminer. Cette conscience, à l'égard des professionnels de la banque, se traduit par la méconnaissance du devoir professionnel de respecter le secret[77].

Comme tout délit, la violation du secret professionnel se prescrit par six ans[78] à compter de la date de la commission du délit.

1.6.3 - Les sanctions disciplinaires

L'Autorité de contrôle prudentiel et de résolution (ACPR) doit s'assurer, en vertu de l'article L.612-1 I du Code monétaire et financier, du respect par les établissements de crédit des dispositions figurant

[77] *Notons l'arrêt de la Cour d'Appel de Grenoble, daté du 9 février 2000, qui a admis que le délit ne puisse être retenu à l'encontre d'un professionnel de la banque qui n'avait pas conscience de communiquer les informations couvertes par le secret (Grenoble, 9 février 2000, JCP 2001. IV. 1464).*

[78] *Article 8 du Code de procédure pénale.*

dans le même Code. En cas de violation du secret bancaire, les sanctions disciplinaires que l'ACPR est en droit de prononcer sont, en conséquence, les suivantes[79] :

- l'avertissement ;
- le blâme ;
- l'interdiction d'effectuer certaines opérations pour une durée maximale de dix ans ;
- la suspension temporaire de dirigeants pour une durée maximale de dix ans ;
- la démission d'office de dirigeants ;
- le retrait partiel ou total d'agrément ou d'autorisation ;
- la radiation de la liste des personnes agréées.

À la place ou en sus de ces sanctions, peut également être prononcée une sanction pécuniaire d'au plus 100 millions d'euros[80].

Lorsqu'il existe des éléments susceptibles de fonder leur responsabilité directe et personnelle[81] dans la violation du secret professionnel, l'ACPR peut également prononcer des sanctions disciplinaires à l'égard des dirigeants de l'établissement (notamment leur suspension temporaire ou leur démission d'office). Une sanction pécuniaire peut être prononcée à la place ou en sus de ces sanctions.

Précisons enfin que la violation du secret bancaire est susceptible de constituer une cause réelle et sérieuse de licenciement dans la mesure où cette violation matérialise un manquement du salarié à ses obligations professionnelles en raison de l'emploi occupé[82].

1.7 - Étude synthétique sur l'encadrement du secret bancaire au sein de plusieurs pays de l'Union européenne, en Suisse et aux États-Unis

Une étude synthétique portant sur l'encadrement juridique du secret bancaire a été réalisée dans certains États membres de l'Union européenne, ainsi qu'en Suisse et aux États-Unis. Cette étude

[79] *Article L.612-1, II, 3°, alinéa 2, et article L.612-39 du Code monétaire et financier. Au jour de la rédaction du présent rapport, le groupe de travail n'avait connaissance d'aucune sanction disciplinaire prononcée par l'ACPR pour violation du secret professionnel.*

[80] *Articles L.612-39 et L.612-41 du Code monétaire et financier.*

[81] *Art. L612-39, alinéa 12, du Code monétaire et financier : « Lorsque la procédure de sanction engagée peut conduire à l'application de sanctions à des dirigeants, la formation de l'Autorité qui a décidé de l'engagement de la procédure indique expressément, dans la notification de griefs, que les sanctions mentionnées aux 4° et 5° sont susceptibles d'être prononcées à l'encontre des dirigeants qu'elle désigne, en précisant les éléments susceptibles de fonder leur responsabilité* ***directe et personnelle*** *dans les manquements ou infractions en cause, et la commission des sanctions veille au respect à leur égard du caractère contradictoire de la procédure.»*

[82] *Paris, 12 octobre 2017, n° 16/01912.*

figure en *Annexe n° 2*. Sur les dix juridictions étudiées, il apparaît que le secret bancaire ne fait l'objet de dispositions légales spécifiques de nature pénale que pour quatre d'entre elles uniquement (au sein de l'Union européenne (UE) : l'Espagne, le Luxembourg et la Pologne ; hors UE : la Suisse).

ll convient de noter qu'en Allemagne, les agents des banques qui relèvent du secteur public sont soumis à un secret professionnel général qui n'est toutefois pas spécifique au secteur bancaire. Sa violation est sanctionnée pénalement. Dans la plupart des cas, la sanction consiste en une peine d'emprisonnement et/ou une amende, de durée et de montants variables. La sanction peut concerner la banque ou ses dirigeants.

Dans les autres juridictions (Allemagne, pour ce qui concerne les banques relevant du secteur privé, Belgique, Italie, Pays-Bas, Royaume-Uni et États-Unis), la protection du secret bancaire ne fait l'objet ni de dispositions légales ou réglementaires, ni de sanctions spécifiques, et découle généralement du droit des contrats, des usages bancaires ou encore de la coutume.

Aucune des juridictions étudiées ne prévoit de sanction disciplinaire spécifique au cas de violation du secret professionnel ou d'une obligation de confidentialité.

1.8 - Premier constat : la difficile appréhension du périmètre du secret bancaire

Les décisions de jurisprudence ayant prononcé les sanctions pénales prévues pour violation du secret bancaire, tout comme le prononcé de sanctions disciplinaires, demeurent rares et les tribunaux se contentent, en règle générale, de peines d'amende pour des montants bien en deçà des *maxima*.

Néanmoins, l'existence même d'une sanction pénale, le caractère personnel de l'infraction, le risque d'interdiction professionnelle et les quelques décisions existantes[83] justifient la préoccupation et la vigilance constante des établissements assujettis en la matière.

Dans ce contexte, force est de constater que l'appréhension du périmètre précis d'application du secret bancaire n'est facilitée ni par la dissémination dans les textes des nombreuses dérogations au secret bancaire, ni par le manque de précisions sur les informations couvertes par le secret. Cette situation demeure source d'insécurité juridique, tant pour les établissements assujettis (et les personnes personnellement responsables) que pour les personnes protégées.

[83] *Notamment : Bourges, 31 octobre 1991, n° 048594 (condamnation à une amende de 5 000 francs) ; Rennes, 13 janvier 1992, RG n° 48/92 (condamnation de 10 000 francs ; Toulouse, 2 décembre 1999, RG n° 99/00155, JCP 2000. IV. 2369 ; Crim. 30 janvier 2001, n° 00-80.367 (condamnation à une amende de 15 000 francs).*

Compte tenu de ce foisonnement d'exceptions au sein de multiples textes, le groupe de travail a estimé qu'il serait souhaitable de procéder à une rationalisation des textes en vigueur **en rassemblant, au sein d'un corpus unique et cohérent, l'ensemble des dérogations au secret bancaire et en apportant les précisions textuelles nécessaires à la détermination des informations couvertes par le secret.**

Il est ainsi préconisé qu'un travail doctrinal réunisse l'ensemble des exceptions au secret bancaire, la création d'un ouvrage par la Doctrine lui apparaissant plus approprié qu'une réforme législative, eu égard à la multitude de textes et de régimes applicables (cf. *Recommandation n° 1*).

II- La difficile conciliation entre secret bancaire et droit à la preuve

Les établissements assujettis sont très souvent confrontés, dans un cadre précontentieux ou contentieux, à la question de l'articulation du secret bancaire avec le droit à la preuve.

Si le secret bancaire est en principe opposable au juge civil et commercial dans la mesure où aucune exception légale n'est prévue par l'article L.511-33 du Code monétaire et financier, la jurisprudence a toutefois dégagé plusieurs exceptions et défini, en dernier lieu par deux arrêts de la chambre commerciale respectivement de 2018 et 2019[84], de nouveaux critères.

L'examen de la typologie des hypothèses de confrontation du secret bancaire avec le droit à la preuve (2.1) constitue un préalable indispensable pour comprendre les difficultés d'application de ces nouveaux principes jurisprudentiels par les établissements assujettis (2.2) et imaginer des solutions alternatives adaptées (2.3).

2.1 - La typologie des hypothèses de confrontation du secret bancaire avec le droit à la preuve

Afin de mieux cerner les cas d'espèce auxquels les établissements assujettis sont confrontés, il convient d'en identifier les principaux caractères distinctifs (2.1.1) et d'en exposer les exemples récurrents (2.1.2).

[84] *Com., 4 juill. 2018, n°17-10.158 ; Com., 15 mai 2019, n°18-10.491.*

2.1.1 - Les caractères distinctifs principaux

L'examen des cas de figure rencontrés révèle au moins cinq caractères distinctifs :

1- Il peut s'agir d'une offre ou une demande de preuve. L'hypothèse selon laquelle l'établissement assujetti offre de communiquer des preuves comportant des informations couvertes par le secret bancaire correspond à une offre de preuve. Lorsqu'un tiers ou un client de l'établissement assujetti sollicite de sa part la communication de preuves comportant des informations couvertes par le secret bancaire, il s'agit d'une demande de preuve.

2- La preuve sollicitée ou proposée comporte des informations concernant le client de l'établissement assujetti ou un tiers à cette relation. L'immense majorité des cas de figure concerne naturellement des éléments de preuve concernant le client de la banque : opérations réalisées par le client figurant sur des relevés de compte, document de demande de financement, courriers adressés par la banque à son client, etc. La communication peut toutefois concerner des tiers à la relation entre l'établissement assujetti et son client : on pense essentiellement à l'hypothèse des informations figurant au verso des chèques qui a fait l'objet d'une jurisprudence abondante, mais il peut s'agir, de manière plus générale, de tout élément d'information concernant un tiers recueilli par l'établissement assujetti à l'occasion d'une opération de paiement ou de financement.

3- La demande ou l'offre de production de pièces couvertes par le secret bancaire est formulée avant tout procès ou au cours d'un procès. C'est l'hypothèse des demandes formulées dans le cadre du référé *in futurum* de l'article 145 du Code de procédure civile (avant procès) et de celles présentées au cours de la procédure au fond devant le Juge de la mise en état ou la formation de jugement (au cours du procès).

4- L'établissement assujetti est partie ou non à un litige. Il peut se voir demander la communication de preuves comportant des informations couvertes par le secret bancaire, sans toutefois être partie à un litige. L'article 11 du Code de procédure civile offre en effet aux parties à un litige la faculté de demander au juge d'ordonner, au besoin sous astreinte, la production de tous documents détenus par des tiers, et donc notamment un établissement assujetti, s'il n'existe pas d'empêchement légitime. La question est alors de déterminer si la protection des données personnelles recueillies par l'établissement constitue l'empêchement légitime prévu par le texte.

5- Dans le cadre du contentieux considéré, l'établissement assujetti est susceptible d'être demandeur ou défendeur au fond. Il est demandeur au fond lorsque, notamment, il sollicite le recouvrement d'une créance, le paiement d'une indemnisation, la reconnaissance et l'exécution d'un droit. Il est en revanche défendeur lorsqu'il a été assigné par son client ou un tiers qui réclame l'exécution d'une prestation ou l'octroi de dommages et intérêts en réparation d'un préjudice.

La combinaison de ces principaux caractères distinctifs se concrétise par des situations contentieuses distinctes multiples.

2.1.2 - Les cas de figure récurrents

Plusieurs cas de figure récurrents peuvent être observés et notamment les hypothèses suivantes :

1- L'établissement assujetti entend obtenir, par la voie judiciaire, le recouvrement de l'une de ses créances auprès de l'un de ses clients et produit, à cet effet, l'acte juridique et les échanges sur lesquels sont fondés sa demande de paiement de la créance dont il est titulaire ; il s'agit d'une offre de preuve comportant des informations concernant le client de l'établissement assujetti, formulée au cours d'un procès dirigé par l'établissement demandeur au fond contre son client. La question du secret bancaire se pose au moins en théorie dans la mesure où les éléments couverts par le secret bancaire seront versés aux débats devant une juridiction civile ou commerciale pour laquelle il n'existe pas d'exception légale à la confidentialité prévue par l'article L.511-33 du Code monétaire et financier.

2- L'établissement assujetti entend obtenir, par la voie judiciaire, le recouvrement de l'une de ses créances à l'encontre d'une caution ; il s'agit là encore d'une offre de preuve comportant des informations concernant le client de l'établissement assujetti, formulée au cours d'un procès dirigé cette fois-ci par l'établissement assujetti demandeur au fond contre un tiers à la relation bancaire.

3- À la suite d'une fraude aux moyens de paiement et préalablement à tout procès en responsabilité, le client d'un établissement assujetti initie à son encontre un référé *in futurum* afin d'obtenir la production d'éléments d'information concernant l'auteur potentiel de la fraude dont il serait victime, comme par exemple les informations figurant au verso d'un chèque falsifié ; le cas de figure correspond alors à une demande de preuve comportant des informations concernant un tiers à la relation bancaire, dans le cadre d'une procédure en référé engagée avant tout procès en responsabilité à l'encontre de l'établissement assujetti.

4- Dans le cadre d'un procès en responsabilité engagé par l'un de ses clients sur un fondement extracontractuel ou contractuel, l'établissement assujetti entend, pour sa défense, produire aux débats des éléments concernant son client couverts par le secret bancaire ; cette hypothèse classique correspond à une offre de preuve comportant des informations concernant le client de l'établissement de crédit dans le cadre d'un procès au fond engagé à son encontre par son client.

5- L'établissement assujetti est assigné en responsabilité par un tiers à la relation bancaire sur le fondement d'un manquement qu'il aurait commis aux engagements précontractuels ou contractuels qui le lient à son client ; on pense notamment aux conséquences pour un tiers créancier du client de l'établissement assujetti de la distribution d'un financement ou la rupture de celui-ci ; il s'agit dans cette hypothèse d'une demande de preuve comportant des informations concernant le client de l'établissement assujetti dans le cadre d'un procès au fond engagé à son encontre par un tiers.

La combinaison des caractères distinctifs principaux évoqués plus haut est susceptible de donner lieu à des situations très variées qui appellent des solutions de règlement adaptées du conflit entre le secret bancaire et le droit à la preuve.

2.2 - Une jurisprudence difficile à mettre en œuvre par les établissements assujettis

2.2.1 - La jurisprudence antérieure

La jurisprudence antérieure aux solutions nouvelles est foisonnante et n'a jamais cessé d'évoluer. Si le principe de l'opposabilité du secret au juge civil ou commercial a été réaffirmé à de multiples reprises, plusieurs exceptions jurisprudentielles ont toutefois vu le jour.

Son examen permet de dégager les principes suivants :

- L'établissement dont la responsabilité est recherchée par son client dispose de la faculté de produire aux débats les éléments couverts par le secret qui sont nécessaires à sa défense[85].

- Par ailleurs, l'établissement assujetti, partie au litige, peut opposer le secret à tout tiers à la relation bancaire dans le cadre d'une demande de preuve. Le secret bancaire ne cesse pas du seul fait que la banque est partie au procès[86].

- Dans le même sens, lorsque la banque est tiers au litige, le secret bancaire auquel elle est tenue constitue un empêchement légitime au sens de l'article 145 du code de procédure civile opposable au juge civil[87].

- Il était également jugé que même lorsque la banque est partie au litige et que la communication par le demandeur a pour objet d'apporter la preuve des manquements qu'elle a commis, elle ne peut être relevée du secret bancaire qui constitue un empêchement légitime, dès lors que son contradicteur n'est pas le bénéficiaire du secret[88].

- Cela étant, l'établissement assujetti ne peut opposer le secret bancaire à la caution et ses ayants droit pour refuser de leur communiquer des informations relatives au débiteur principal, dès lors qu'il appartient au banquier d'établir l'existence et le montant de la créance dont il réclame le paiement[89].

Deux arrêts, rendus respectivement en 2017 et 2018, sans doute annonciateurs de la nouvelle jurisprudence, ont toutefois décidé que lorsqu'un procès est intenté contre une banque par un tiers à la relation bancaire (client d'une autre banque ou caution au titre d'un engagement consenti par

[85] *CA Paris, 23 mai 1996, RDBB 1996, 236, obs. F.-J. Crédot et Y. Gérard.*

[86] *Com., 13 juin 1995, n° 93-16.317 ; Com. 25 févr. 2003, n° 00-21.184 ou encore Com. 21 févr. 2012, n° 11-10.900.*

[87] *Com., 25 févr. 2003, n° 00-21.184 ; Com. 21 sept. 2010, n° 09-68.994 ; Com., 21 févr. 2012, n° 11-10.900.*

[88] *Com., 13 nov. 2003, n° 00-19.573 ; Com., 25 janv. 2005, n° 03-14.693 ; Com., 5 févr. 2013, n° 11-22.746.*

[89] *Com., 16 déc. 2008, n° 07-19.777.*

l'établissement assujetti), en vue de rechercher l'éventuelle responsabilité de l'établissement, ce dernier ne peut opposer le secret bancaire pour refuser de communiquer des informations concernant son client qui pourrait permettre de démontrer sa responsabilité[90].

La difficulté d'interprétation des décisions de jurisprudence est renforcée à raison du fait que les textes du Code de procédure civile ont une valeur réglementaire alors que le secret bancaire repose sur un fondement législatif.

2.2.2 - Les nouvelles conditions dégagées par la jurisprudence de la chambre commerciale de la Cour de cassation

2.2.2.1 - Le contexte européen

Le contexte européen est déterminant pour comprendre l'évolution de la jurisprudence de la chambre commerciale de la Cour de cassation.

Plusieurs décisions de la Cour de Justice de l'Union européenne (CJUE) et de la Cour Européenne des Droit de l'Homme (CEDH) ont en effet recherché un équilibre entre le respect à la vie privée et l'exercice du droit à la preuve par l'instauration d'un contrôle de proportionnalité[91]. Dans son rapport annuel 2012, la Cour de cassation relève que ce contrôle est fondé sur « *un rapport de proportionnalité entre les intérêts que le secret protège et ceux à la satisfaction desquels il fait obstacle, dès lors que, dans cette mise en balance, l'atteinte au secret paraît moindre, et constituer le seul moyen de faire triompher une légitime prétention au fond* »[92].

Un arrêt remarqué de la CJUE a ainsi condamné, s'agissant du droit de propriété qui était en conflit avec le secret bancaire, l'autorisation de ne pas communiquer les informations couvertes par ledit secret dès lors que cette autorisation est illimitée et inconditionnelle[93].

La voie était donc ouverte pour une redéfinition par la Cour de cassation des conditions d'articulation du secret bancaire avec le droit à la preuve.

2.2.2.2 - L'évolution de la jurisprudence de la chambre commerciale

Par deux arrêts, la chambre commerciale a redéfini les principes applicables permettant la conciliation du secret bancaire avec le droit à la preuve.

---

[90] *Com. 29 nov. 2017, n° 16-22.060 ; Com., 24 mai 2018, n° 17-27.969.*

[91] *CEDH, 10 oct. 2006, n° 7508/02, L. L. c/ France ; CEDH, 13 mai 2008, n° 65097/01, N. N. et T. A. c/ Belgique.*

[92] *C. Cass. Rapp. Annuel 2012 : La preuve dans la jurisprudence, p.329.*

[93] *CJUE, 16 juill. 2015, aff. C-580/13, Coty Germany.*

Dans une première affaire, une banque avait été assignée par une cliente en restitution de sommes correspondant au montant d'opérations réalisées au moyen de sa carte bancaire. La banque avait versé aux débats les relevés du compte dont sa cliente était titulaire sur une période de plus d'un an et demi afin de démontrer que les opérations objet du litige étaient habituelles et s'opposer aux demandes de remboursement formées à son encontre. La Cour d'appel avait écarté ces relevés de compte des débats au motif qu'aucun élément ne lui permettait de lever le secret bancaire. La chambre commerciale, par une décision du 4 juillet 2018, a toutefois cassé l'arrêt rendu en appel en soulignant qu'en se « *déterminant ainsi, sans rechercher si la production litigieuse n'était pas indispensable à l'exercice par la banque de son droit à la preuve et proportionnée aux intérêts antinomiques en présence, la cour d'appel a privé sa décision de base légale* »[94].

La seconde affaire portait sur le contentieux classique de la demande formée par des clients, dans le cadre d'un référé *in futurum*, de la production du verso de plusieurs chèques potentiellement frauduleux en vue de la mise en cause ultérieure de la responsabilité de leur banquier. En appel, la Cour avait retenu, selon la solution classique en la matière, que la banque pouvait valablement refuser de communiquer le verso des chèques en opposant le secret bancaire à ses clients. Là encore, la chambre commerciale a cassé l'arrêt de la Cour par une décision du 15 mai 2019, au motif « *qu'en se déterminant ainsi, sans rechercher si la communication à M. et Mme R. des informations figurant au verso des chèques qu'ils avaient émis n'était pas indispensables à l'exercice de leur droit à la preuve, pour rechercher l'éventuelle responsabilité de la banque lors de l'encaissement desdits chèques, et proportionnée aux intérêts antinomiques en présence, incluant la protection du secret dû aux bénéficiaires de ces chèques, la cour d'appel a privé sa décision de base légale* »[95].

Confronté au secret bancaire, l'exercice du droit à la preuve est donc soumis à deux conditions cumulatives. Il convient en effet d'apprécier si la production des éléments couverts par le secret bancaire est :

- en premier lieu, indispensable à l'exercice du droit à la preuve de la partie formulant la demande ou l'offre de preuve ;

- en second lieu, proportionnée aux intérêts antinomiques en présence, incluant la protection du secret dû à son bénéficiaire.

---

[94] *Com., 4 juill. 2018, n° 17-10.158 ; N. Mathey, Chronique Droit bancaire n° 1596, JCP E, p.36 ; J. Lasserre Capdeville, Le secret bancaire face au droit à la preuve, JCP E, n° 40, 4 oct. 2018, 1507 ; RD banc. Fin., n° 6, nov.-déc. 2018, Droit bancaire, comm. T. Samin et S. Torck.*

[95] *Com., 15 mai 2019, n° 18-10.491 ; Th. Bonneau, Le secret bancaire face au « droit à la preuve », JCP G, n° 24, 17 juin 2019, p.1143 ; H. Michelin-Brachet, Droit à la preuve et secret bancaire : le délicat arbitrage, D. 2019, p.1595 ; Medhi Kebir, Droit à la preuve et levée du secret bancaire : contrôle de proportionnalité, D. actu. 17 juin 2019 ; Chronique sous la direction de Nicolas Mathey, JCP E, n° 47, 21 nov. 2019, 1528, n° 4, p.3 ; D. R. Martin et H. Synvet, Droit bancaire juillet 2018 – septembre 2019, D. 2019, p.2009.*

Cette solution a été appliquée à deux espèces bien distinctes au regard des caractères distinctifs principaux exposés plus haut :

- dans la première affaire (décision du 4 juillet 2018), il s'agissait d'une offre de preuve formulée par un établissement assujetti dans le cadre d'un procès en cours afin de faire échec à une action en remboursement de sommes d'argent initiée à son encontre par l'un de ses clients, étant précisé que les informations dont la production était proposée concernaient ce dernier et potentiellement, s'agissant de relevés de compte, des tiers à la relation bancaire ;

- dans la seconde affaire (décision du 15 mai 2019), il s'agissait d'une demande de preuve formulée par un client de la banque dans le cadre d'un référé *in futurum* afin d'obtenir des informations concernant un tiers à la relation bancaire.

On peut donc penser que pour la chambre commerciale, la solution qu'elle propose a une vocation universelle. Elle serait donc susceptible de recevoir application à l'ensemble des hypothèses de confrontation du secret bancaire avec le droit à la preuve déjà évoquées.

2.2.2.3 - Analyse des deux conditions cumulatives retenues par la chambre commerciale

Les deux conditions cumulatives appellent les observations suivantes.

La production doit tout d'abord être « *indispensable à l'exercice du droit à la preuve* ». Le droit à la preuve est tiré de l'article 6 de la Convention européenne des droits de l'Homme et constitue donc un droit fondamental. Il renvoie à la faculté pour le justiciable d'une part d'obtenir des preuves (demande de preuve) et d'autre part de produire des preuves (offre de preuve).

Pour l'essentiel, la preuve demandée ou offerte doit être pertinente. Cette caractéristique résulte de l'application combinée des articles 6 et 9 du code de procédure civile.

L'article 6 du code de procédure civile prévoit que :

« *À l'appui de leurs prétentions, les parties ont la charge d'alléguer les faits propres à la fonder.* »

L'article 9 du code de procédure dispose pour sa part que :

« *Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention.* »

Autrement formulé, si la partie concernée doit indiquer les faits sur lesquels ses prétentions sont fondées, encore faut-il que ces faits soient réellement « *nécessaires au succès de ses prétentions* ». Le

plaideur n'aura aucune raison valable de produire des éléments de preuve s'ils ne sont pas susceptibles d'avoir une influence sur la décision attendue[96]. Dans ce contexte, le terme de pertinence « *s'entend, essentiellement, de la pertinence de l'allégation des faits qui doit tomber directement sur l'espèce et de la pertinence de la preuve qui doit conduire à une démonstration appropriée* », étant précisé que « *la pertinence est, dans les deux cas, souverainement appréciée par le juge* »[97]. Certains auteurs ne manquent pas de relever que « *si cette règle est évidente, la notion de pertinence manque néanmoins de précision* »[98] et c'est d'ailleurs bien la raison pour laquelle son appréciation relève du pouvoir souverain des juges du fond lorsque leur conviction dépend du fait considéré[99].

Non seulement la production envisagée doit porter sur une preuve pertinente, mais encore faut-il, selon la chambre commerciale, qu'elle soit indispensable à l'exercice du droit à la preuve. Cela signifie que la production doit constituer pour le plaideur le seul moyen d'apporter la preuve du fait allégué de sorte qu'il « *ne suffit pas que la preuve produite soit utile ; elle doit être la seule possible* »[100].

La production des éléments couverts par le secret bancaire doit en outre être proportionnée aux intérêts antinomiques en présence. Il appartient alors de procéder à une mise en balance d'une part de l'intérêt à la protection des données personnelles protégées par le secret bancaire et d'autre part de l'intérêt matériel défendu par le droit à la preuve.

La chambre commerciale de la Cour de cassation ne fournit toutefois aucune précision sur les modalités de mise en œuvre de ce contrôle de proportionnalité. Dans la première affaire ayant donné lieu à la décision du 4 juillet 2018, la chambre commerciale invite la Cour de renvoi à mettre en regard l'intérêt pour la banque d'éviter que sa responsabilité ne soit engagée d'une part et l'intérêt pour sa cliente de ne pas voir divulguée une série d'informations figurant sur les relevés du compte dont elle est titulaire d'autre part. Dans l'arrêt du 15 mai 2019, il s'agit d'apprécier l'intérêt pour les clients de rechercher la responsabilité de l'établissement assujetti au regard de l'intérêt des tiers bénéficiaires de chèques, voire des tiers les ayant endossés successivement, de ne pas voir révélées les informations les concernant figurant au verso de formules de chèque.

En l'absence de mode d'emploi, il semble que l'établissement bancaire astreint au secret est invité à procéder à une appréciation *in concreto* des intérêts antinomiques en présence selon des critères non explicités fortement liés à l'espèce considérée.

Le contrôle proposé par la chambre commerciale se démarque donc par une grande subjectivité.

---

[96] *H. Motulsky, Principes d'une réalisation méthodique du droit privé, thèse, Lyon, 1947, n° 84 s.*

[97] *S. Guinchard et G. Montagnier, Lexique de termes juridiques, Dalloz, 9e édition, p.398.*

[98] *G. Lardeux, Preuve : règles de preuve, Répertoire de droit civil, n° 71.*

[99] *Civ. 2e, 30 janv. 1980, n° 79-12.470.*

[100] *G. Lardeux, Le droit à la preuve : tentative de systématisation, RTD Civ. 2017, p.1.*

2.2.3 - Des principes difficiles à mettre en œuvre par l'établissement assujetti

Les hypothèses extrêmement variées de conflit entre le secret bancaire et le droit à la preuve que les établissements sont susceptibles de rencontrer ont été précédemment décrites.

La chambre commerciale les invite à confronter les cas de figure ainsi recensés à sa nouvelle grille de lecture. L'on s'aperçoit toutefois rapidement que les principes ainsi dégagés sont difficiles à mettre en œuvre par les établissements assujettis.

Prenons l'exemple visé *supra* du client d'un établissement assujetti qui initie à son encontre un référé *in futurum* afin d'obtenir la production d'éléments d'information concernant l'auteur potentiel d'une fraude.

À titre préalable, il convient de rappeler que dans cette hypothèse, l'établissement qui s'opposerait indûment à la production sollicitée s'exposerait à une condamnation à prendre en charge les frais de procédure de son adversaire, voire à l'indemniser des conséquences de son abstention injustifiée de communiquer les éléments demandés.

L'application des principes dégagés par la chambre commerciale impliquerait donc pour l'établissement souhaitant éviter toute condamnation de :

- dans un premier temps, s'assurer que la production de pièces qui lui est demandée est indispensable à l'exercice au droit à la preuve de son client ; il doit donc déterminer si les éléments sollicités sont nécessaires au succès des prétentions que le client n'a pas été en mesure de formuler expressément, puisque sa demande est formée au moyen d'un référé *in futurum* avant tout procès au fond. L'établissement assujetti devra en outre vérifier que les éléments demandés par son client sont indispensables, c'est-à-dire qu'il ne disposait d'aucune autre possibilité d'apporter la preuve des faits venant au soutien de ses prétentions. N'ayant aucune certitude sur les éléments détenus ou non par son client, cette vérification est très difficilement réalisable par l'établissement assujetti.

- dans un second temps, procéder à un contrôle de proportionnalité entre des intérêts qui ne lui sont pas directement propres, soit d'une part l'intérêt de son client à rechercher sa responsabilité de banquier et d'autre part l'intérêt de tiers à la relation bancaire de voir protéger leurs données personnelles couvertes par le secret bancaire. Aucun critère objectif n'étant fixé par la jurisprudence, l'établissement assujetti devra donc privilégier une approche *in concreto* nécessairement empreinte de subjectivité.

Les établissements assujettis sont donc confrontés à des difficultés importantes pour mener à bien le contrôle défini par la chambre commerciale et préfèreront vraisemblablement éviter le reproche de violation du secret bancaire au risque d'une condamnation à une indemnisation prononcée sur le plan civil. La prudence n'est toutefois d'aucun secours pour l'établissement dont la responsabilité est mise en cause qui entend produire des éléments nécessaires à sa défense, mais couverts par le

secret. Dans cette hypothèse, l'établissement concerné devra choisir entre le risque de violer le secret bancaire et l'impossibilité de se défendre pour échapper à la mise en cause de sa responsabilité.

2.3 - Proposition de solutions alternatives

Certaines situations contentieuses appellent indiscutablement une levée du secret bancaire afin de permettre l'exercice du droit à la preuve en dehors du contrôle de proportionnalité désormais prévu par la jurisprudence de la chambre commerciale.

Est concerné l'ensemble des hypothèses à l'occasion desquelles l'établissement assujetti entend produire, dans le cadre d'un contentieux l'opposant à son client, des informations le concernant.

Dit autrement, ces cas de figure appartiennent à l'ensemble défini par les caractères distinctifs suivants :

- l'établissement assujetti formule une offre de preuve ;
- il est partie à un litige ;
- ce litige l'oppose à son client ;
- les informations couvertes par le secret bancaire concernent son client ;
- l'offre de preuve est formulée avant ou au cours d'un procès.

Les hypothèses appartenant à cet ensemble correspondent essentiellement à l'offre de preuve formulée par :

- l'établissement assujetti demandeur à une action afin d'obtenir la reconnaissance d'un droit ou le paiement d'une créance (ex : action en recouvrement engagée par l'établissement assujetti contre son client emprunteur) ;

- l'établissement assujetti défendeur à une action afin d'échapper à la mise en cause de sa responsabilité (ex : action en responsabilité engagée par le client contre son établissement).

Dans ces cas de figure, il est nécessaire, afin de permettre à l'établissement assujetti de se défendre, de le délier du secret bancaire auquel il est astreint pour lui permettre de faire valoir ses droits à l'encontre de son client. Il est possible en effet de considérer que le client a consenti au moins implicitement à la levée du secret bancaire dans la limite du différend l'opposant à son banquier. Celui-ci doit pouvoir, afin de faire valoir ses droits, opposer à son client des éléments le concernant couverts par le secret[101]. Il faut néanmoins, dans cette hypothèse, que la preuve soit, dans les termes de l'article 9 du code de procédure civile, nécessaire au succès des prétentions de l'établissement assujetti. L'établissement assujetti pourra s'affranchir du secret bancaire uniquement si les éléments qu'il produit aux débats sont pertinents au regard des prétentions qu'il formule.

Dans cette hypothèse, l'établissement assujetti serait donc dispensé :

- d'apporter la démonstration du caractère indispensable de la preuve proposée,
- et de réaliser le contrôle de proportionnalité des intérêts antinomiques en présence.

L'article L.511-33 du Code monétaire et financier ne prévoit toutefois pas d'exception au secret bancaire et précise au contraire qu'en dehors des cas spécifiques de levée, la communication d'informations couvertes n'est possible « *uniquement lorsque les personnes concernées leur ont expressément permis de le faire* ».

Il conviendrait donc d'ajouter à l'article L.511-33 du Code monétaire et financier un alinéa complémentaire afin de couvrir l'hypothèse d'une levée du secret en cas de procédure judiciaire entre les établissements assujettis et leurs clients afin de permettre à l'établissement d'exercer pleinement les droits de la défense (cf. *Recommandation n° 2*).

En dehors de ces hypothèses, les nouveaux principes arrêtés par la chambre commerciale trouveraient à s'appliquer.

Il paraît en effet logique que la production d'informations couvertes par le secret concernant un client dans le cadre d'un litige à l'occasion duquel l'établissement assujetti est opposé à un tiers à la relation bancaire ou encore la production d'informations concernant un tiers à la relation bancaire dans le cadre d'un litige opposant cet établissement à son client soit soumise à un contrôle plus strict.

Néanmoins, la tentative d'application des critères dégagés par la chambre commerciale à des cas concrets montrent les difficultés auxquelles est confronté l'établissement assujetti qui ne dispose pas des moyens d'apprécier si la preuve demandée ou proposée est indispensable à l'exercice du droit à la preuve et encore moins le caractère proportionné aux intérêts antinomiques en présence de la production envisagée.

En réalité, seul le juge saisi du litige à l'occasion duquel la demande ou l'offre de preuve est formulée dispose de la connaissance nécessaire du litige sous-jacent et des moyens pour procéder à ce contrôle.

Il conviendrait de tirer toute conséquence de ce constat en offrant aux parties de faire trancher la difficulté par le juge dans un cadre procédural adapté. La partie sollicitant ou proposant la production des éléments couverts par le secret serait invitée à solliciter l'autorisation préalable du juge.

---

[101] *CA Paris, 23 mai 1996 : JurisData n° 1996-021442 ; RD bancaire et bourse 1996, p.236, col. 1, obs. F.-J. Crédot et Y. Gérard.*

Un dispositif similaire, prévu par les articles L.153-1 et 153-2 du Code de commerce, existe déjà en matière de secret des affaires ; **il pourrait être adapté au secret bancaire (cf. *Recommandation n° 3).***

III- De nouvelles exceptions au secret bancaire pour répondre aux difficultés opérationnelles des établissements assujettis

L'organisation des établissements assujettis et leur environnement réglementaire a significativement évolué depuis la dernière réforme du secret bancaire : recours croissant à la sous-traitance, notamment informatique, diversification des activités, renforcement de leurs obligations (notamment en matière de sécurité financière), filialisation et spécialisation des entités au sein des groupes bancaires, etc. La transmission des informations couvertes par le secret est devenu un prérequis indispensable au fonctionnement normal et régulier des établissements.

Dans ce contexte, il est apparu au groupe de travail que des évolutions ciblées au régime du secret bancaire pourraient être envisagées afin de lever un certain nombre de difficultés opérationnelles rencontrées par les établissements assujettis. Trois domaines ont ainsi été identifiés concernant les relations entre les établissements assujettis et leurs sous-traitants (3.1), certains impératifs légaux et réglementaires s'imposant aux banques (3.2) et la protection des intérêts des clients (3.3).

3.1 - Secret bancaire et sous-traitants de la banque

L'article L.511-33-I du Code monétaire et financier, 3e alinéa, 6° dispose que les établissements de crédit peuvent communiquer des informations couvertes par le secret professionnel « *aux personnes avec lesquelles ils négocient, concluent ou exécutent* » certaines opérations, dès lors que ces informations sont nécessaires à celles-ci, en particulier en cas de « *contrats de prestations de services conclus avec un tiers en vue de lui confier des fonctions opérationnelles importantes* ».

La notion approximative de « *fonctions opérationnelles importantes* » ne correspond à aucune qualification connue en droit bancaire. On comprend toutefois que cette notion fait écho à la notion de « *tâches opérationnelles essentielles ou importantes* » utilisée par l'arrêté du 3 novembre 2014[102] pour définir le périmètre des activités externalisées (articles 10 q) et10 r) de l'arrêté).

[102] *Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution définit les prestations de services ou autres tâches opérationnelles essentielles ou importantes.*

Le champ de la sous-traitance bancaire dépassant largement le seul cadre des activités essentielles externalisées (par exemple la sous-traitance des fonctions juridiques, comptables, la facturation, les ressources humaines, ou encore les achats de prestations standard), **il est recommandé de supprimer la notion de « fonctions opérationnelles importantes » de l'article L.511-33, 3e alinéa, 6°, du Code monétaire et financier (cf. *Recommandation n° 4*).**

Du point de vue des clients cette suppression ne présenterait pas de risques car l'article L.511-33, al. 5 du Code monétaire et financier garantit en toute hypothèse leur protection en disposant que les tiers qui reçoivent des informations couvertes par le secret dans le cadre d'un contrat de prestation de services, doivent les conserver confidentielles, que l'opération aboutisse ou non. Cette protection est à ce titre assurée par l'insertion dans les contrats de sous-traitance de clauses ou d'accords de confidentialité ad hoc. De nombreux contrats de prestations de services visent à servir l'intérêt du client : le secret bancaire ne doit pas être un frein à l'externalisation de services qui sont utiles à ce dernier.

3.2 - Secret bancaire et impératifs réglementaires

3.2.1 - Secret bancaire et Agence Française Anticorruption

L'Agence française anticorruption (AFA) est un service à compétence nationale créé par la loi du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite « loi Sapin 2 »).

Placée auprès du ministre de la Justice et du ministre en charge du Budget, elle aide les autorités compétentes et les personnes qui y sont confrontées à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme. Son expertise peut être sollicitée par les juridictions, les grandes entreprises, les administrations ou encore les collectivités.

L'AFA est dirigée par un magistrat de l'ordre judiciaire hors hiérarchie[103] nommé par décret du président de la République pour une durée de six ans non renouvelable. L'Agence française anticorruption a remplacé le Service central de prévention de la corruption (SCPC) tout en bénéficiant d'un renforcement de ses pouvoirs.

L'Agence française anticorruption dispose d'un pouvoir administratif de contrôle lui permettant de vérifier la réalité et l'efficience des mécanismes de conformité anticorruption mis en œuvre,

[103] *Monsieur Charles Duchaine au jour de la publication du présent rapport.*

notamment par les entreprises, les administrations de l'État ou les collectivités territoriales. Ce contrôle concerne aussi bien les administrations de l'État ou les collectivités territoriales que les acteurs économiques (entreprises privées ou publiques)[104].

Dans le cadre uniquement de ces contrôles des dispositifs de conformité des établissements assujettis, l'AFA peut demander des informations couvertes par le secret bancaire aux établissements assujettis. Or à la différence de ce qui a été prévu pour la Haute Autorité pour la transparence de la vie publique (ci-après la « HATPV ») qui « *peut se faire communiquer, sur pièce, par les représentants d'intérêts, toute information ou tout document nécessaire à l'exercice de sa mission, sans que le secret professionnel puisse lui être opposé* »[105], la loi Sapin 2 n'a pas envisagé explicitement de dérogation au secret bancaire au profit de l'AFA dans le cadre de ses pouvoirs de contrôle. En effet, l'article 4 de la loi dispose que :

« *Dans le cadre de ses missions définies aux 3° et 4° de l'article 3, les agents de l'Agence française anticorruption peuvent être habilités, par décret en Conseil d'État, à se faire communiquer par les représentants de l'entité contrôlée tout document professionnel, quel qu'en soit le support, ou toute information utile. Le cas échéant, ils peuvent en faire une copie.*

Ils peuvent procéder sur place à toute vérification de l'exactitude des informations fournies. Ils peuvent s'entretenir, dans des conditions assurant la confidentialité de leurs échanges, avec toute personne dont le concours leur paraît nécessaire. Les agents habilités, les experts et les personnes ou autorités qualifiées auxquels ils ont recours et, de manière générale, toute personne qui concourt à l'accomplissement des missions mentionnées à l'article 3 sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont connaissance en raison de leurs fonctions, sous réserve des éléments nécessaires à l'établissement de leurs rapports. »

La loi ne comporte donc aucune disposition déclarant que le secret professionnel ne peut pas être opposé à l'AFA dans le cadre de ses missions de contrôle des dispositifs de conformité des établissements assujettis. Or, telle semblait bien être l'intention du législateur. Le rapport au Sénat de M. Pillet précise ainsi que :

« *L'article 4 du projet de loi vise à instaurer pour les membres de l'Agence de prévention de la corruption, un droit de communication par les représentants de toute entité contrôlée, applicable de tout document professionnel ou à toute information utile et la possibilité de s'entretenir, de manière confidentielle, avec toute personne dont le concours apparaît nécessaire.*

---

[104] *Cette présentation de l'AFA peut être retrouvée sur son site : https://www.agence-francaise-anticorruption.gouv.fr/fr/lagence.*

[105] *Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite « Sapin 2 », art. 25.*

Ce droit de communication s'inspire de dispositions similaires à l'instar du droit de communication de l'administration fiscale prévu ***aux articles L. 81*** *et suivants du livre des procédures fiscales ou de celui de l'administration des douanes prévu* ***aux articles 64 A*** *et suivants du code des douanes.* ***Il vise à permettre aux agents de ne pas se voir opposer le secret professionnel.***

Considérant, à l'instar du Conseil d'État dans son avis sur le projet de loi, que l'habilitation des fonctionnaires de l'agence à se faire communiquer ces documents relève d'un décret en Conseil d'État *(…)* »[106]

Aussi, afin de lever toute ambiguïté et de clarifier sans aucun doute possible que, lors des contrôles de l'AFA portant sur un établissement assujetti, le secret bancaire ne peut lui être opposé par celui-ci, il est proposé **une clarification des textes par le biais d'une modification ciblée de l'article L.511-33 du Code monétaire et financier qui serait de nature à permettre une communication des éléments demandés relevant du secret bancaire (cf. *Recommandation n° 5*)**. Le groupe de travail a en effet considéré que l'ajout d'une nouvelle exception au secret bancaire relève du domaine législatif et non pas d'un décret en Conseil d'État.

Il convient de souligner que lorsque les agents de l'AFA interviennent dans le cadre d'un contrôle de CJIP (Convention Judiciaire d'Intérêt Public), ils agissent alors pour le compte du Parquet National Financier ; il peut dès lors être soutenu qu'ils bénéficient des mêmes droits d'accès que les autorités judiciaires agissant dans le cadre d'une procédure pénale.

3.2.2 - Secret bancaire et lutte contre le blanchiment et le financement du terrorisme

Les banques ont des obligations de vigilance dans le domaine de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Ces obligations sont prévues aux articles L.561-2 à L.561-50 et R.561-1 à R.561-64 du Code monétaire et financier.

La mise en œuvre des obligations de vigilance par les banques peuvent les conduire à adresser à Tracfin, la cellule de renseignement financier de la France, une déclaration de soupçon conformément à l'article L.561-15 du Code monétaire et financier qui dispose que les banques doivent déclarer à Tracfin les sommes ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme.

[106] *Sénat, « Rapport n° 712 : Projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique » (2015-2016) de M. François PILLET, fait au nom de la commission des lois, déposé le 22 juin 2016, < http://www.senat.fr/rap/l15-712-1/l15-712-110.html#toc75>.*

Les déclarations de soupçon qui sont transmises à Tracfin sont analysées et, éventuellement, enrichies par les investigations de Tracfin pour, le cas échéant, être adressées aux administrations « partenaires » de Tracfin pour suite à donner. Il s'agit, notamment, des autorités judiciaires (juridictions et services d'enquêtes judiciaires) ; des services de renseignements ; de l'administration fiscale ; des URSSAF.

Pour être correctement exploitées par Tracfin, il est très important que les déclarations de soupçon adressées à Tracfin soient les plus circonstanciées possibles.

Actuellement, les situations complexes de blanchiment de capitaux ou de financement de terrorisme sont difficiles à capter en raison, notamment, des limitations à l'échange d'informations sur les déclarations de soupçon entre banques n'appartenant pas au même groupe.

En particulier, il est souhaité que les banques n'appartenant pas au même groupe puissent avoir la possibilité de s'échanger des informations pour les besoins de la surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme lorsqu'elles sont désignées dans le cadre du droit au compte par la Banque de France (cf. *Recommandation n° 6*). Cela permettrait à la banque désignée de mettre en place une vigilance appropriée dans les meilleurs délais.

En effet, les personnes désignées au titre du droit au compte peuvent voir leur compte fermé pour des motifs de conformité en lien, notamment, avec la lutte contre le blanchiment de capitaux ou le financement du terrorisme. Il est important pour qu'une surveillance efficace puisse être mise en œuvre immédiatement que la banque désignée au titre du droit au compte puisse avoir des informations sur les incidents de conformité qui ont pu conduire à la cessation de la relation contractuelle avec le client.

3.3 - Secret bancaire et protection des intérêts des clients ou de tiers

3.3.1 - Secret bancaire et rappel de produits dangereux

Lorsqu'un consommateur a acquis un produit dont il s'avère, ultérieurement, qu'il peut présenter des dangers pour la santé, le commerçant n'a pas la possibilité de prendre contact avec les clients potentiellement concernés, car il ne dispose que d'un numéro de carte/opération bancaire (il n'a pas nécessairement l'adresse postale ou les coordonnées téléphoniques de son client). Ce dernier doit, en effet, être en possession de ces éléments pour prévenir l'acquéreur du produit qu'il ne doit pas l'utiliser et le restituer sans délai.

Sauf si la convention de compte autorise une telle communication, il ne reste que la possibilité de lever le secret bancaire en raison d'un texte spécifique afin de transmettre les données strictement

nécessaires à la protection des personnes concernées (nom, prénom, numéro de téléphone, adresse email, adresse postale, etc.). Or en l'état actuel des textes aucune exception au secret bancaire n'est prévue.

Concernant la règlementation en matière de données personnelles, le RGPD[107] dispose dans son article 6 d) qu'un traitement est licite s'il est nécessaire « *à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique* ». Dans un avis de 2014, le G29 précise que, dans le cadre de la réglementation sur la protection des données, ce fondement s'applique aux « *questions de vie ou de mort, ou, à tout le moins, à des menaces qui comportent un risque de blessure ou une autre atteinte à la santé de la personne concernée* »)[108].

Dès lors que cette transmission de données a pour but de sauvegarder les intérêts vitaux de la personne dans la limite des données strictement nécessaires à la réalisation de cette finalité, le consentement du porteur n'est pas nécessaire et ce dernier ne bénéficie pas du droit de s'opposer au traitement au regard du RGPD[109].

Par analogie, concernant le secret bancaire, **la loi pourrait prévoir que les établissements assujettis pourront communiquer des informations de contact des clients dont ils disposent, couvertes par le secret professionnel, aux distributeurs, dans le cadre d'un rappel de produits, si ces derniers confirment qu'elles sont nécessaires à la sauvegarde des intérêts vitaux de la personne concernée (l'utilisateur de services de paiement) ou d'une autre personne physique** (ses proches - **cf. *Recommandation n° 7***). Une définition très large de l'intérêt vital serait dans ces conditions nécessaire. Une définition de la sauvegarde des intérêts vitaux conforme à l'avis de 2014 pourrait être prévue dans les textes. Cette définition sera applicable spécifiquement à cette nouvelle dérogation au secret bancaire et il faudra la distinguer de la notion voisine issue du RGPD.

En raison de la finalité de la communication, de l'urgence et du caractère restreint du nombre de données transmises, à l'instar de ce qui est prévue pour la réglementation sur la protection des données, aucune possibilité ne devrait être offerte au consommateur de s'opposer à la transmission de ces données. À défaut, il pourrait en résulter des conséquences dommageables pour l'efficacité pratique d'un tel dispositif.

---

[107] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données, ou « règlement général du la protection des données » (ci-après « RGPD »).*

[108] *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, p. 22.*

[109] *Article 21.1 du RGPD.*

Finalement, la banque devrait pouvoir se fier uniquement aux informations fournies par les producteurs et les distributeurs pour savoir s'il est nécessaire ou non de transmettre les données aux distributeurs. En effet, en aucun cas cette dernière ne possède la compétence pour se faire juge de la dangerosité du produit justifiant la communication des données. Le banquier ne devrait également être tenu de ne transmettre que les données dont il dispose à l'exclusion de toute autre.

Étant donné le risque d'image pour les producteurs et les distributeurs qu'entraîne un rappel de produit, il est probable que ces derniers ne demanderont la communication des données que dans les cas le justifiant c'est-à-dire à titre exceptionnel.

3.3.2 - Secret bancaire et protection des personnes vulnérables

La personne dont il va être question ci-après est une personne capable mais dont les facultés mentales peuvent être plus ou moins fortement altérées par l'effet, par exemple, de l'âge. Il s'agit donc d'un majeur capable qui ne fait l'objet, par hypothèse, d'aucune mesure de protection. Le banquier ne peut donc pas s'opposer à la libre disposition de ses fonds.

L'article 430 du Code civil prévoit que :

« *La demande d'ouverture de la mesure peut être présentée au juge par la personne qu'il y a lieu de protéger ou, selon le cas, par son conjoint, le partenaire avec qui elle a conclu un pacte civil de solidarité ou son concubin, à moins que la vie commune ait cessé entre eux, ou par un parent ou un allié, une personne entretenant avec le majeur des liens étroits et stables, ou la personne qui exerce à son égard une mesure de protection juridique.*

Elle peut être également présentée par le procureur de la République *soit d'office, soit* ***à la demande d'un tiers.*** »

Ce texte laisserait donc la possibilité au banquier de saisir le procureur de la République. En effet, les personnes qui n'ont pas qualité à agir (au sens du premier alinéa de l'article 430 du Code civil) peuvent donner avis au procureur de la République de la cause qui justifierait la mesure de protection. Ce dernier appréciera, le cas échéant, après enquête et après avoir fait procéder aux vérifications médicales nécessaires, la suite à donner.

Il existe des arguments forts pour considérer que le banquier fait partie des personnes qui peuvent effectuer un signalement au procureur de la République.

3.3.2.1 - Un argument principal : le secret est édicté dans l'intérêt du client

Cette opinion s'appuie sur l'ouvrage de M. Massip[110] dans lequel il est indiqué (n° 280 p. 234) :

« *Parmi les personnes pouvant être amenées à donner un tel avis figurent le médecin traitant du malade, les services sociaux qui ont pu être appelés à intervenir, les responsables de l'établissement de*

*traitement, **ainsi que les banquiers** et les notaires (13)* »

Le Conseiller à la Cour de cassation semble ainsi considérer que le secret bancaire est en l'occurrence levé. Ce que semble confirmer la note 13 auquel renvoie le corps du texte :

« *V. p. ex. Cass. civ. 1e, 25 mai 1992, Defr. 30 novembre 1992, n° 22, p.1445, obs. J. Massip ; adde sur le secret professionnel des notaires en matière de protection des majeurs, TGI La Roche-sur-Yon, 3 avril 1990, Defr. 1993, art. 35572, n° 53, obs. J. Massip.* »

Remarque : l'arrêt et le jugement cité concernent le secret professionnel des notaires. M. Massip assimile le secret bancaire et le secret professionnel des notaires[111].

L'idée sous-jacente du Haut Conseiller est que le secret professionnel est conçu dans l'intérêt du client. Or, en l'occurrence, l'intérêt du majeur est que le confident nécessaire (notaire, banquier) parle en ne donnant que les informations strictement indispensables au procureur de la République. Dans ces conditions, il est donc possible de donner des informations nominatives au procureur de la République.

3.3.2.2 - Premier argument subsidiaire : l'ordre de la loi

La loi du 23 mars 2019 a modifié l'article 431 du Code civil. Le dernier alinéa de cet article prévoit désormais que

« *Lorsque le procureur de la République est saisi par une personne autre que l'une de celles de l'entourage du majeur énumérées au premier alinéa de l'article 430, la requête [en vue d'une protection juridique d'un majeur,] transmise au juge des tutelles comporte en outre, à peine d'irrecevabilité, les informations dont cette personne dispose sur la situation sociale et pécuniaire de la personne qu'il y a lieu de protéger et l'évaluation de son autonomie ainsi que, le cas échéant, un bilan des actions personnalisées menées auprès d'elle. La nature et les modalités de recueil des informations sont définies par voie réglementaire. Le procureur de la République peut solliciter du tiers qui l'a saisi des informations complémentaires.* »

Il pourrait être considéré que l'article 431 du Code civil prévoit la remise d'informations sur la situation pécuniaire du majeur à protéger, or l'article 122-4 du Code pénal, relatif à l'ordre de la loi dispose que :

« *N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires.* »

---

[110] *Jacques Massip, Tutelle des mineurs et protection juridique des majeurs, Éditions Defrénois/Lextenso, mai 2009.*

[111] *V. aussi en ce sens : Massip, note sous Cass. Civ. 1e, 22 mai 2002, pourvoi n° 00-16.305, Petites Affiches n° 46 du 5 mars 2003, p. 19.*

3.3.2.3 - Second argument subsidiaire : l'état de nécessité[112]

Aux termes de l'article 121-7 du Code pénal : « *N'est pas pénalement responsable la personne qui, face à un danger actuel ou imminent qui menace elle-même, autrui ou un bien, accomplit un acte nécessaire à la sauvegarde de la personne ou du bien, sauf s'il y a disproportion entre les moyens employés et la gravité de la menace* ». La caractérisation de cette cause d'irresponsabilité pénale implique une triple preuve :

- l'existence d'un péril actuel ou imminent ;
- l'acte commis doit être indispensable pour éviter le péril ;
- l'intérêt sauvegardé a une valeur plus importante que l'intérêt sacrifié.

Ces trois conditions sont bien présentes dans le cas qui nous intéresse :

- si des prélèvements inhabituels ont été opérés sur le compte de la personne en situation de faiblesse, ou des paiements réalisés à partir de ce même compte, nous sommes bien en présence d'un danger actuel concernant ses biens ;

- l'information du procureur est indispensable pour mettre un terme à un tel danger (à titre d'exemple, si les chèques ont bien été signés par la victime ou que les prélèvements sont opérés par l'intermédiaire de sa carte bancaire avec tabulation du code secret, la banque ne peut guère s'opposer à de telles opérations) ;

- l'intérêt sauvé, c'est-à-dire la préservation de l'intégrité du patrimoine de la victime, est plus important que la discrétion entourant ce dernier.

3.3.2.4 - En dernier lieu, on peut relever que, dans certaines circonstances, le respect d'une prescription légale ou réglementaire (dans l'ordre juridique français) peut constituer une cause d'irresponsabilité pénale

En effet, aux termes de l'article 122-4, alinéa 1er, du Code pénal, l'ordre ou l'autorisation de la loi peut constituer une cause objective d'irresponsabilité pénale. En d'autres termes, les faits commis ne revêtent plus de caractère délictuel et ne peuvent entrainer une condamnation pénale, quand bien même les éléments constitutifs de l'infraction seraient caractérisés. (« *N'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires* »).

[112] *V. en ce sens J. Lasserre-Capdeville, « Le banquier face au délit d'abus de faiblesse », Revue de Droit bancaire et financier n° 5, Septembre 2012, étude 24.*

Bien qu'il n'a pas été identifié de jurisprudence traitant spécifiquement de la justification d'une violation du secret bancaire par l'application des obligations s'imposant à des établissements de crédit ou des entreprises d'investissement (par exemple, des obligations de reporting, résultant notamment de textes européens comme MiFID/MiFIR ou encore REMIT ou SFTR), il est possible de considérer que si des poursuites pour violation du secret bancaire étaient déclenchées le prestataire bancaire ou financier pourrait vraisemblablement invoquer avec succès l'autorisation de la loi résultant du texte concerné dans la mesure où :

- il n'est pas requis que les dispositions utilisées pour justifier le délit soient de nature pénale. Par ailleurs, elles peuvent être issues d'une règle de droit international ayant force obligatoire en France (par exemple, un traité ratifié par la France ou un règlement européen, d'application directe dans l'ordre juridique français). À titre d'exemple, une jurisprudence ancienne de la chambre criminelle a déjà confirmé que l'application d'une règle de droit communautaire pouvait justifier la commission d'une infraction (il s'agissait d'une infraction à la législation règlementant la publicité en faveur des boissons alcoolisées, Crim. 16 juin 1983, n°81-92316, Bull. Crim. 1983[113]). En revanche, l'excuse de la loi ne peut certainement pas être invoquée lorsque l'obligation résulte d'un texte étranger n'ayant pas force obligatoire en France. Selon une ancienne jurisprudence relative à l'article 122-4 du code pénal en effet, « *l'ordre prétendu de la loi étrangère ne saurait être invoqué comme fait justificatif lorsque le délit poursuivi a été commis sur le territoire français* » (Cass. Crim., 27 juin 1973, n° 73-90057) ; et

- il n'est pas nécessaire que les dispositions invoquées prévoient expressément qu'elles constituent une exception aux dispositions pénales (ici, au secret bancaire), l'autorisation peut en résulter implicitement[114].

Traditionnellement, la jurisprudence concernant l'article 122-4 du Code pénal exige, pour retenir l'autorisation de la loi, que l'acte commis respecte les limites des prescriptions légales et soit nécessaire. Au cas d'espèce, cette exigence signifierait que la banque ou l'entreprise d'investissement ne doit pas avoir communiqué des informations couvertes par le secret mais non concernées par les obligations légales ou réglementaires en cause (ou dont la divulgation n'était pas prescrite par les dispositions concernées).

Cela étant dit, comme il s'agit ici d'appliquer un principe général de droit pénal qui n'est pas spécifique à la matière bancaire et financière et qui, à la connaissance du groupe de travail, n'a pas donné lieu

[113] *Dans cette affaire, l'infraction consistait en un délit de publicité illégale d'une boisson alcoolisée.*

[114] *Ce principe général est en effet plus large que l'article L. 226-14 du code pénal qui précise que le secret professionnel ne s'applique pas dans les cas où la loi impose ou autorise la révélation du secret.*

à des décisions judiciaires publiées le mettant en œuvre dans un tel contexte, ses contours sont toujours évidemment difficiles à appréhender avec certitude. Dans ce contexte, **le rapport préconise que l'analyse qui est développée supra soit confirmée par une circulaire du Ministère de la Justice (cf. *Recommandation n° 8*)**.

IV- Une clarification et une rationalisation souhaitables des exceptions existantes au secret bancaire

4.1 - Secret bancaire et opérations de M&A bancaire

4.1.1 - Contexte

De prime abord, les articles L.511-33 et L.522-19 du Code monétaire et financier, applicables respectivement aux établissements de crédit et aux entreprises d'investissement[115], prévoient des exceptions permettant la transmission d'informations confidentielles dans le cadre d'opération de M&A dans le secteur financier, dans les cas suivants :

- prises de participation ou de contrôle dans un établissement de crédit, une entreprise d'investissement ou une société de financement ;
- cessions d'actifs ou de fonds de commerce ; et
- cessions ou transferts de créances ou de contrats.

Selon le texte, les informations peuvent ainsi être transmises aux personnes avec lesquelles les établissements « négocient, concluent ou exécutent » ces opérations, dès lors que ces informations sont nécessaires à celles-ci.

4.1.2 - Difficultés pratiques

Pour autant, malgré cela, le texte se révèle inadapté en pratique, notamment dans les opérations de prise de participation ou de contrôle, pour les raisons suivantes.

[115] *Ainsi qu'aux sociétés de financement.*

En premier lieu, au regard personnes concernées :

(i) tout d'abord, les parties à l'opération sont l'acquéreur et le vendeur. Or les informations couvertes par le secret professionnel sont celles dont la cible est le dépositaire, tandis que c'est l'actionnaire cédant sa participation[116] qui souhaite donner accès à ces informations à l'acquéreur. Et ce n'est d'ailleurs pas non plus la cible qui négocie avec l'acquéreur les modalités de sa cession ;

(ii) ensuite, l'acquéreur de la participation (plus particulièrement lorsqu'il s'agit d'un fonds d'investissement) n'est pas, bien souvent, la personne qui négociera effectivement les termes de l'acquisition : l'acquéreur sera juridiquement une société holding spécialement constituée pour l'occasion (holdco, newco, bidco, etc.), tandis que l'acquisition sera négociée avec le sponsor ou gérant du fonds, parfois bien avant que la holding soit même créée ; et

(iii) enfin, l'exception ne s'étend pas aux différents conseils (cabinets d'audit et de conseil, conseil financier, cabinets d'avocats, etc.), qui assistent tant le vendeur (notamment dans la constitution et la gestion de la dataroom virtuelle) que l'acquéreur, voire aux financiers de l'acquéreur (et leurs conseils respectifs). Or ces derniers peuvent avoir accès aux informations confidentielles.

Le texte prévoit certes la possibilité pour les personnes ayant reçu des informations couvertes par le secret de les transmettre à leur tour à des tiers. Mais cette faculté n'est offerte que lorsque l'opération d'acquisition aura abouti, or c'est en amont même de la phase de négociation qu'il peut s'avérer nécessaire de transmettre de telles informations, notamment par l'acquéreur, à ses conseils[117]. Au surplus, une telle transmission ne peut intervenir qu'à l'occasion d'une des opérations visées par l'article L. 511-33. Les autres exceptions ne sont guère plus utiles[118].

En second lieu, se pose la question du moment de l'entrée en *négociation* des termes de l'opération d'acquisition, afin de bénéficier de l'exception au secret bancaire. Typiquement, une opération d'acquisition s'articule généralement autour de plusieurs phases, à savoir :

(i) une première phase, aux termes de laquelle le vendeur met à la disposition des acquéreurs potentiellement intéressés des informations concernant la cible leur permettant de formuler une manifestation d'intérêt indicative ;

---

[116] *Et qui n'est pas nécessairement un établissement de crédit ou une société de financement ou encore une entreprise d'investissement.*

[117] *Article L. 511-33-I, al. 6 : « Toutefois, dans l'hypothèse où l'opération susvisée aboutit, ces personnes peuvent à leur tour communiquer les informations couvertes par le secret professionnel dans les mêmes conditions que celles visées au présent article aux personnes avec lesquelles elles négocient, concluent ou exécutent les opérations énoncées ci-dessus. »*

[118] *Article L. 511-33-I, 6° « Contrats de prestations de services conclus avec un tiers en vue de lui confier des fonctions opérationnelles importantes » et 7° « Lors de l'étude ou l'élaboration de tout type de contrats ou d'opérations, dès lors que ces entités appartiennent au même groupe que l'auteur de la communication ».*

(ii) puis une seconde phase, au cours de laquelle une information plus précise et détaillée est mise à la disposition d'une population plus restreinte d'acquéreurs potentiels, afin de permettre à ces derniers de formuler une offre comportant un prix ; et

(iii) enfin, une troisième phase, au cours de laquelle le vendeur entre en négociation exclusive avec un acquéreur potentiel et qui se termine par la signature du contrat d'acquisition.

À quel moment la négociation de l'opération débute-t-elle ? Et donc, à quel moment, au regard des phases décrites ci-dessus, une information couverte par le secret professionnel peut-elle transmise à l'acquéreur ?

Enfin, on peut douter du fait que l'entrée en négociation constitue le moment pertinent à partir duquel des informations confidentielles peuvent être partagées. En effet, n'existe-t-il pas, avant ce moment, une période durant laquelle l'acquéreur potentiel doit apprécier la qualité de la cible et procéder à l'étude du dossier ? Par conséquent, **il est proposé, l'instar de ce que prévoit déjà le paragraphe 7° de l'article L. 511-33 du Code monétaire et financier, de permettre la divulgation d'informations couvertes par le secret lors de l'élaboration ou l'étude des opérations qui sont visées dans la liste mentionnée au I de l'article L.511-33 (cf. *Recommandation n° 9*).**

4.1.3 - Risque pénal partagé

Dans ce contexte, le risque de sanction pénale est partagé entre les différents protagonistes, à savoir :

(i) l'établissement cible, au titre de la violation du secret professionnel ;

(ii) le vendeur (ainsi que, éventuellement, ses conseils lorsque ces derniers ont pris une part active dans la mise à disposition et la transmission des informations), au titre de la complicité de violation du secret professionnel[119] ; et

(iii) enfin, l'acquéreur potentiel et les conseils professionnels (tant de l'acquéreur que du vendeur), au titre, le cas échéant, du recel d'informations couvertes par le secret[120].

[119] *Article 121-7 du code pénal: « Est complice d'un crime ou d'un délit la personne qui sciemment, par aide ou assistance, en a facilité la préparation ou la consommation. »*

[120] *Article 321-1 du code pénal: « Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit ». Pour autant toutefois que l'information soit transmise sous forme documentaire.*

4.1.4 - Anonymisation des informations : une solution de portée limitée

Une solution pratique généralement mise en œuvre dans les opérations d'acquisitions de banques consiste à anonymiser les informations mises à disposition des acquéreurs potentiels et leurs conseils.

Cette solution convient généralement dans le cadre de la première phase d'accès à la dataroom, car les informations qui y sont contenues sont généralement également sous forme agrégées.

En revanche, elle trouve sa limite dès la deuxième phase, car elle ne répond que très imparfaitement aux nécessités de l'opération (par exemple, l'évaluation des risques de crédit sur la clientèle de la cible). En outre, elle se heurte à des difficultés pratiques la rendant onéreuse et difficile à réaliser (anonymisation des contrats et des dossiers de crédit relatifs à des volumes importants de crédits, tels que les crédits à la consommation).

Au final, il est préconisé une **évolution de l'article L.511-33 du Code monétaire et financier pour pallier les lacunes du texte (cf. *Recommandation n° 9*).**

4.2 - Une clarification nécessaire de certaines exceptions

4.2.1 - Opérations de crédit (paragraphe 1° de l'article L.511-33-I)

Les opérations de crédit[121] relèvent du monopole des établissements de crédit et des sociétés de financement prévu à l'article L.511-5 du Code monétaire et financier. Par conséquent, il semble de prime abord logique de limiter le bénéfice de l'exception au secret bancaire relatif aux opérations de crédit aux seuls établissements de crédit et aux sociétés de financement fournissant un crédit à l'établissement de crédit qui, à cette fin, leur communique des informations confidentielles. Cependant, cette logique est mise à mal par le nombre croissant d'exceptions qui se sont développées depuis 2008[122]. Par conséquent, il devient absurde, d'un côté, de permettre à des personnes qui ne sont pas des établissements de crédit, ni des sociétés de financement, de réaliser des opérations de crédit avec de tels établissements ou sociétés et, de l'autre, de les priver de l'accès aux informations couvertes par le secret professionnel qui sont pourtant nécessaires à la réalisation de ces opérations.

[121] *Définies à l'article L.313-1 du Code monétaire et financier.*

[122] *V. articles L.511-6 et L.511-7 du Code monétaire et financier. Est en particulier visée, à titre d'exemple, l'exception relative à la cession de créances bancaires à des organismes étrangers introduite par la loi Sapin II au §4° de l'article L. 511-6 du Code monétaire et financier.*

Par conséquent, dans un souci de cohérence, **il est proposé de supprimer la référence aux établissements de crédit et aux sociétés de financement au paragraphe 1° de l'article L. 511-33-I (cf. *Recommandation n° 10-a*).**

4.2.2 - Opérations de couverture du risque de crédit (paragraphe 2° de l'article L.511-33-I)

Le paragraphe 2° de l'article L.511-33-I du Code monétaire et financier permet à un établissement de crédit ou une société de financement, dans le cadre d'opérations de couverture du risque de crédit relatif à ses actifs, de divulguer des informations relatives à ces actifs qui sont couvertes par le secret professionnel. Cependant, à l'épreuve de la pratique, cette exception souffre de plusieurs défauts.

En premier lieu, un établissement de crédit ou une société de financement est exposée à d'autres risques que le seul risque de crédit, pour la couverture desquels une protection, de nature financière ou assurantielle, peut être recherchée[123]. Or la mise en place d'une telle couverture peut nécessiter la transmission d'informations couvertes par le secret professionnel au fournisseur de protection.

En second lieu, la précision quant à l'*instrumentum* utilisé pour opérer le transfert de risques est peu opportune, compte tenu de la variété des instruments potentiellement utilisés, et peut être vue comme inutilement restrictive, d'autant plus dans l'hypothèse d'un élargissement des types de risques potentiellement couverts. Au surplus, on peut hésiter sur la question de savoir si certaines techniques de gestion de la couverture de risques (par exemple, dans le cadre de « *macro-hedging* » de portefeuilles d'investissements ou d'actifs) relèvent bien de la notion de « couverture » qui reste imprécise.

Par conséquent, **il est proposé, au paragraphe 2° de l'alinéa 3 l'article L.511-33-I, de supprimer la référence aux instruments financiers, aux opérations de garanties ou d'assurance et de préciser que ces opérations sont destinées à la couverture ou à la gestion de tous risques (cf. *Recommandation n° 10-b*).**

4.2.3 - Opérations intra-groupes (paragraphe 7° de l'article L.511-33-I)

L'article L.511-33 du Code monétaire et financier, 3e alinéa, 7° dispose que les établissements de crédit peuvent communiquer des informations « *lors de l'étude ou de l'élaboration de tout type de contrats ou d'opérations, dès lors que ces entités appartiennent au même groupe que l'auteur de la communication.* »

[123] *Voir l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution, qui vise par exemple, le risque de marché, de liquidité, d'intermédiation ou encore le risque opérationnel.*

Si le début du 3e alinéa permet de comprendre que cette dérogation s'étend à la négociation, la conclusion ou l'exécution de certaines opérations dont la liste suit (et inclut celles visées au paragraphe 7°), il en résulte une incohérence textuelle, puisque le paragraphe 7° ne vise que l'étude ou l'élaboration [de tout type de contrats…], mais pas leur exécution, ce qui semble donc restreindre le champ du paragraphe 3 lui-même.

Quand bien même la logique du texte commande d'inclure l'exécution du contrat (on ne comprendrait pas pourquoi la divulgation d'informations couvertes par le secret bancaire serait permise lors de l'élaboration du contrat, mais pas à l'occasion de son exécution), cette **incohérence textuelle mériterait d'être corrigée, en cohérence avec les modifications proposées dans le cadre de la Recommandation n° 9, afin que la dérogation relative aux contrats et opérations intra-groupes s'étende, sans doute possible, à l'exécution et à la gestion de ces opérations ou contrats (cf. *Recommandation n° 10-c*).**

4.2.4 - Opérations pour les besoins de la fourniture de services à la clientèle (ajout d'un (paragraphe 8° nouveau à l'article L. 511-33-I)

Alors que la réalisation de prestations bancaires (au sens large) par les banques à leurs clients peuvent impliquer la fourniture de services par un certain nombre de prestataires, relevant de la profession bancaire ou non (établissements de crédit/sociétés de financement, établissements de paiement ou de monnaie électronique, entreprises d'assurance, entreprises d'investissement, sociétés de gestion de portefeuille, etc.), lesquels devront souvent pouvoir disposer de l'accès à des informations couvertes par le secret professionnel de la banque afin d'exécuter leur propres obligations.

Or il n'existe aucune exception utile qui puisse justifier l'existence d'un « secret partagé » entre acteurs concernés en matière bancaire et financière. Une telle exception semble donc nécessaire afin de sécuriser la banque dans ses relations avec les prestataires avec lesquels elle va contracter afin de fournir ses propres services ou une panoplie de services à ses clients grâce au concours d'autres prestataires fournissant leurs propres services de manière coordonnée.

Par conséquent, **il est proposé d'ajouter un nouveau paragraphe 8° à l'article L. 511-33-I, permettant la transmission d'informations confidentielles dans le cadre d'opération de banque, de paiement, de monnaie électronique ou toute autre opération, effectuée pour les besoins de la fourniture des services à la clientèle (cf. *Recommandation n° 10-d*).**

4.2.5 - Règlement STS (ajout d'un 5e alinéa nouveau à l'article L. 511-33-I)

Les titrisations ne sont pas couvertes par le texte actuel. Alors que le règlement (UE) No. 2017/2402 du parlement européen et du conseil du 12 décembre 2017 créant un cadre général pour la titrisation ainsi qu'un cadre spécifique pour les titrisations simples, transparentes et standardisées impose des obligations de transparence à l'égard des investisseurs qui ne sont pas toujours compatibles avec le secret bancaire, aucune disposition spécifique n'est prévue par ce règlement pour relever les banques initiatrices de leur obligation de confidentialité.

À l'instar de ce que prévoit le 4e alinéa de l'article L.511-33 du Code monétaire et financier relatif à la transmission d'informations à un référentiel central étranger, il est par ailleurs utile d'étendre l'exception aux titrisations qui devraient obéir à des législations étrangères similaires.

Une exception similaire n'a, en revanche, pas semblé utile au groupe de travail pour les besoins de l'émission de *covered bonds* dans la mesure où, selon le modèle de structuration français, les créances bancaires sont apportées par la banque en garantie d'un prêt qui lui est accordé par un établissement de crédit affilié, agréé sous la forme d'une société de crédit foncier (SCF) ou d'une société de financement de l'habitat (SFH), lequel émet des obligations foncières. Les investisseurs n'ont généralement pas accès à des informations individualisées concernant le portefeuille de créances entrant dans l'assiette de la sûreté et, partant, il ne semble pas exister de difficultés au regard du secret bancaire.

Par conséquent, **il est proposé d'insérer un nouvel alinéa à l'article L.511-33-I, à la suite de l'actuel 4e alinéa, permettant la transmission d'informations confidentielles dans le cadre du règlement STS ou d'une législation étrangère équivalente (cf. *Recommandation n° 10-e*).**

4.3 - Le cas des services électroniques de stockage et de partage de données/ services d'intermédiation électroniques ou « plateformes électroniques »

Un nombre croissant de métiers de la banque doivent recourir à des services d'intermédiaires électroniques (parfois appelés « plateformes électroniques »[124]) qui assurent l'accès aux informations, contenus, services ou biens édités ou fournis par des tiers tant en amont des dossiers, que dans leur phase d'exécution et ce, sans nécessairement avoir de liens contractuels avec ces derniers.

[124] *Ces plateformes ne doivent pas être confondues avec les plateformes de médias sociaux des GAFA.*

L'article L.511-33 du Code monétaire et financier ne traite pas les situations dans lesquelles des informations couvertes par le secret professionnel transitent par ces « plateformes électroniques » et il conviendrait d'y remédier. Cela parait d'autant plus nécessaire que l'utilisation de ces services se développe dans de nombreux domaines de la finance (y compris en particulier dans le domaine des opérations de fusions et d'acquisitions d'établissements dans le secteur financier avec le recours à des prestataires fournissant des services de *data rooms* virtuelles, comme « *Datalink* », ainsi que, de plus en plus fréquemment, dans les opérations de financements ou de refinancement, d'assurances, etc.) et que les incertitudes juridiques qui subsistent exposent les acteurs de ces opérations à des menaces et handicapent la place financière de Paris.

Le dossier mentionné ci-dessous illustre ainsi la problématique à laquelle les banques françaises peuvent être confrontées en matière de secret bancaire lorsqu'elles recourent à ces outils.

Une société met à disposition de ses utilisateurs un outil offrant des services de placement d'assurance sur laquelle des courtiers chargent des informations confidentielles fournies par des établissements de crédit telles que le nom des emprunteurs, les caractéristiques des contrats de crédit (montants, dates de signature, profil de remboursement, etc.) et qui sont ensuite consultables par les assureurs pouvant fournir des assurances de type risque de crédit ou *Credit Risk Insurance* (CRI). Cette plateforme électronique est devenue un point de passage obligé pour obtenir des assurances du type CRI auprès des assureurs. L'objectif principal de ces services est de faciliter la signature par les assureurs des polices de CRI par voie électronique. Une autre société fournit quant à elle l'infrastructure informatique à la plateforme, si bien que cette société comme celle qui met à disposition de ses utilisateurs ces services peuvent avoir accès à ces informations confidentielles.

Si la CRI constitue bien un des types d'« *Opérations […] de garanties ou d'assurance destinées à la couverture d'un risque de crédit* » au sens de l'article L.511-33, 2°, du Code monétaire et financier, aucune de ces deux sociétés ne sont des « *personnes avec lesquelles ils négocient, concluent ou exécutent* » de telles opérations et par conséquent, aucune d'elles ne peut bénéficier de cette dérogation au secret bancaire. En l'absence d'une autorisation expresse fournie par l'emprunteur, il n'existe aucune autre dérogation qui serait applicable à la communication des informations confidentielles sur cette plateforme.

Cette situation n'est pas sans analogie avec des situations décrites dans la partie IV. A. *infra* sur le M&A bancaire pour lesquelles des entités recevant des informations couvertes par le secret professionnel ne sont pas non plus des « *personnes avec lesquelles ils négocient, concluent ou exécutent* » l'opération concernée. Cette situation et cette analyse sont très probablement applicables aux autres plateformes électroniques dont le rôle principal est de fournir un service d'intermédiaire dans l'accès aux informations, contenus, services ou biens édités ou fournis par des tiers entre divers acteurs de marché avec lesquels elles n'ont pas de relations commerciales ou contractuelles.

Les contrats de prêt types de la *Loan Market Association* (LMA) qui servent de standard de marché ne comportent pas de dérogation expresse pour les plateformes électroniques à l'instar de celles existant pour des tiers aux opérations concernées que sont les « fournisseurs de services de codification »[125] et les « services administratifs ou de règlement »[126]. Compte tenu de sa rédaction générale, l'article 35.2(b) (ii)[127] pourrait constituer une exception mais dans la mesure où il est plus libéral que la loi actuelle, il semble qu'il faudrait l'accompagner d'une levée expresse du secret bancaire, sachant que cette levée est commercialement difficile à obtenir et n'intervient souvent qu'avec la signature de la documentation de prêt alors que les démarches CRI peuvent être engagées avant.

À la suite d'une réunion de la LMA qui s'est tenue à Londres en décembre 2019 et au cours de laquelle ce sujet de plateforme électronique a été abordé, la LMA n'a pas souhaité s'engager dans la modification des modèles de contrat et la question reste ouverte.

Dans ces conditions, **l'ajout aux 3e et 6e alinéas de l'article L.511-33-I du Code monétaire et financier d'une mention spécifique aux personnes « *par l'intermédiaire desquelles* » certaines opérations sont négociées, conclues ou exécutées « *ainsi qu'à toute personne leur fournissant une prestation d'assistance ou de conseil financier comptable, juridique ou technique* » en conjonction avec les modifications proposées par ailleurs aux termes de la Recommandation n° 9, permettraient de répondre à cette préoccupation (cf. *Recommandation n° 11*** par renvoi à la recommandation n° 9).

4.4 - L'extension aux nouveaux acteurs

Plusieurs « nouveaux acteurs » réglementés ne semblent pas soumis aux mêmes obligations de secret alors même que ceux-ci exercent des activités assimilables ou similaires à celles qu'exercent par

[125] *Article 35.3 du « Contrat d'ouverture de crédit multidevises comportant un crédit à terme et une ouverture de crédit réutilisable » de février 2020.*

[126] *Article 35.2(c) du même contrat.*

[127] *« 35. 2 Communication d'Information Confidentielle*
Une Partie Financière pourra, sans préjudice des dispositions de l'article L.511-33 du Code monétaire et financier, communiquer : […]
(b) à toute personne : […]
(ii) avec qui (ou par l'intermédiaire de qui) elle conclut (ou peut potentiellement conclure), directement ou indirectement, une opération de sous-participation en relation avec un ou plusieurs Documents de Financement et/ou un ou plusieurs Débiteurs, ou toute autre opération en vertu de laquelle des paiements doivent être faits ou pourront être faits par référence à un ou plusieurs Documents de Financement et/ou un ou plusieurs Débiteurs, ainsi qu'aux Sociétés Affiliées, aux Fonds Liés, aux Représentants et aux conseils professionnels de cette personne. »

ailleurs les établissements assujettis au secret en vertu des articles L.511-33, L.522-19 (établissements de paiement) et L.531-12 (entreprises d'investissement et société de gestion) du Code monétaire et financier. Il en est ainsi des prestataires de services sur actifs numériques (1) ainsi que des intermédiaires en financement participatif et des conseillers en investissement participatif (2).

4.4.1 - Les prestations de services sur actifs numériques

En matière de cryptoactifs, la loi PACTE a introduit en France le statut de prestataire en services sur actifs numériques (« PSAN ») couvrant un grand nombre d'activités :

- la conservation d'actifs numériques pour le compte de tiers (soit en pratique la conservation des clés cryptographiques pour le compte d'un client) ;

- l'achat-vente d'actifs numériques contre une monnaie ayant un cours légal ou contre d'autres actifs numériques (courtage) ;

- l'exploitation d'une plateforme de négociation d'actifs numériques (bourse) ;

- d'autres services sur actifs numériques comme la réception et transmission d'ordres pour le compte de tiers, la gestion de portefeuille pour le compte de tiers, le conseil, la prise ferme, le placement garanti et le placement non garanti.

Les PSAN ne sont pas exemptés d'une obligation à la confidentialité. L'article 721-14 du Règlement général de l'AMF dispose que « *préalablement à la fourniture d'un service sur actifs numériques, le prestataire de services sur actifs numériques conclut une convention écrite […] avec son client* » et que *cette dernière doit notamment contenir des indications sur « [l]es obligations de confidentialité à la charge du prestataire de services sur actifs numériques conformément aux lois et règlements en vigueur relatifs au secret professionnel.* »

Ce renvoi au secret professionnel qui est une obligation légale, par le biais d'un texte réglementaire et sans que soit visé précisément le texte auquel il est fait référence, interroge. Le régime des PSAN étant « calqué » sur celui des entreprises d'investissements (moyennant des adaptations), il serait donc cohérent, que comme ces derniers, ils soient soumis par un renvoi dans la loi aux dispositions sur le secret professionnel de ces dernières.

4.4.2 - Les intermédiaires en financement participatifs et les conseillers en investissement participatif

Selon les dispositions de l'article L.547-1-I du Code monétaire et financier, les conseillers en investissement participatif (« CIP ») sont « *les personnes morales exerçant à titre de profession habituelle une activité de conseil en investissement mentionnée au 5 de l'article L.321-1 portant*

sur des offres de titres de capital et de titres de créance définies par décret […]. L'activité exercée par les conseillers en investissements participatifs porte également sur les offres de minibons mentionnés à l'article L.223-6. Ils exercent alors une activité identique à celle prévue au 5 de l'article L. 321-1 s'agissant des titres financiers. […] ».

Les CIP sont bien soumis à une obligation de confidentialité puisque l'article 325-56 du Règlement général de l'AMF dispose que « *sauf accord exprès du client, le conseiller en investissements participatifs s'abstient de communiquer et d'exploiter, en dehors de sa mission, pour son compte propre ou pour le compte d'autrui, les informations relatives au client qu'il détient du fait de ses fonctions* ».

Néanmoins, dans un souci d'une meilleure protection de la clientèle et de traitement équitable des différents acteurs, il semble peu cohérent de ne pas aligner le régime des CIP sur celui d'autres acteurs soumis au secret qui fournissent, à l'instar des CIP, des services d'investissement.

L'activité d'intermédiaires en financement participatif (« IFP ») est quant à elle définie à l'article L.548-1 du Code monétaire et financier. Elle « *consiste à mettre en relation, au moyen d'un site internet, les porteurs d'un projet déterminé et les personnes finançant ce projet […]* ». Un projet consiste en un achat ou un ensemble d'achats de biens ou de prestations de service concourant à la réalisation d'une opération prédéfinie en termes d'objet, de montant et de calendrier (Art. L.548-1-3° du Code monétaire et financier).

L'article L.548-2 du Code monétaire et financier définit les IFP d'une part comme « *les personnes qui exercent, à titre habituel, l'intermédiation au sens de l'article L.548-1 pour les opérations de prêt à titre onéreux ou sans intérêt* », et d'autre part, comme « *les personnes qui exercent, à titre habituel, l'intermédiation au sens de l'article L.548-1 et qui ne proposent que des opérations de dons sont également intermédiaires en financement participatif* ». L'activité d'IFP porte sur les crédits, les prêts sans intérêts et les dons. Les crédits, dont il est question ici, sont mentionnés au 7 de l'article L.511-6. Il s'agit de prêts rémunérés dans le cadre du financement participatif de projets déterminés, consentis par des personnes physiques agissant à des fins non professionnelles ou commerciales, conformément aux dispositions de l'article L.548-1 et dans la limite d'un prêt par projet. L'article D.548-1, dans sa version actuelle issue du décret n°2016-1453 du 28 octobre 2016, précise que ces derniers ne peuvent excéder 2 000 euros par prêteur et par projet.

L'activité des IFP portant notamment sur des prêts, il semblerait cohérent que leurs opérations soit soumis au secret professionnel dont les contours devraient être adaptés aux particularités de leur activité.

Dans une logique de protection de la clientèle et de traitement équitable des différents acteurs réglementés, **ces « nouveaux acteurs » devraient être soumis au secret professionnel (cf. *Recommandation n° 12*).**

V- L'articulation complexe des dispositions légales encadrant le secret bancaire avec les réglementations récentes

5.1 - Secret bancaire et droit de la protection des données à caractère personnel

Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données, ou « règlement général du la protection des données » (ci-après « RGPD »), est entré en application dans l'ensemble des pays membres de l'Union européenne le 25 mai 2018.

D'application directe en droit local, le RGPD ne nécessitait pas de textes de transposition en droit français. Le législateur français, qui aurait ainsi pu se contenter d'abroger les dispositions anciennes au profit du RGPD, a néanmoins décidé de conserver la loi n° 78-17 du 6 janvier 1978 Informatique et Libertés en modifiant les articles concernés et y en apportant les aménagements nécessaires à sa conformité au droit européen[128].

Si le RGPD n'a pas fondamentalement modifié les principes juridiques français qui préexistaient en matière de protection des Données à Caractère Personnel (ci-après « DCP »), il a néanmoins opéré un renversement dans la logique de responsabilité des acteurs en passant d'un régime de formalités préalables à un principe de responsabilisation des responsables en amont de la mise en place des traitements et tout au long de leur vie (principes d'*accountability,* de *privacy by design* et *by default* notamment). Cette nouvelle logique s'illustre, notamment, par un renforcement très significatif des sanctions encourues par les responsables de traitements en cas de manquement[129].

Le RGPD manifeste également une volonté marquée de renforcer les droits des personnes. C'est à ce titre que le groupe de travail s'est interrogé sur la difficile conciliation entre le secret bancaire et, d'une part, le droit à la portabilité nouvellement introduit par le règlement (5.1.1) et, d'autre part, la notion de consentement à un traitement de DCP (5.1.2).

5.1.1 - Droit à la portabilité et secret bancaire

L'article 20 du RGPD a créé un nouveau droit accordé aux personnes sur leur DCP : le droit à la portabilité. Cet article dispose que :

---

[128] *La loi n° 78-17 du 6 janvier 1978 a ainsi été modifiée par la loi n° 2018-493 du 20 juin 2018 et complétée par deux décrets permettant de finaliser l'harmonisation du droit français aux dispositions européennes (décret n° 2018-687 du 1er août 2018 modifiant le décret n° 2005-1309 du 20 octobre 2005 et décret n° 2019 -536 du 29 mai 2019).*

[129] *De 300 000 € d'amende administrative avant l'entrée en vigueur de la Loi pour une République numérique en 2016, à 3 millions d'euros ensuite, les sanctions maximales ont été portées par la RGPD à 20 millions d'euros et 4% du chiffre d'affaires de l'entité en contravention avec ces dispositions.*

« 1. Les personnes concernées ont le droit de recevoir les données à caractère personne les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :

a) le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou un sur un contrat en application de l'article 6, paragraphe 1, point b) ; et

b) le traitement est effectué à l'aide de procédés automatisés.

2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, ***elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.***

3. L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17 [droit à l'effacement ou à l'oubli]. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement.

4. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers. »

Le G29[130], dans ses Lignes Directrices relatives au droit à la portabilité des données[131], indique que « *ce nouveau droit a pour objectif de responsabiliser les personnes concernées et de leur permettre de contrôler davantage les données à caractère personnel les concernant* ». Le G29 indique en outre que, « *dans la mesure où il permet la transmission directe des données à caractère personnel d'un responsable de traitement à un autre, le droit à la portabilité des données constitue également un instrument important qui facilitera la libre circulation des données à caractère personnel dans l'Union et qui stimulera la concurrence entre les responsables de traitement* ».

Les conditions fixées par l'article 20 du RGPD pour l'exercice du droit à la portabilité ont fait l'objet d'une interprétation extensive au sein de ces mêmes Lignes Directrice. Le G29 considère en effet que :

- les données « *fournies* » doivent couvrir tant les données « *directement et activement* » fournies par la personne concernée (nom, adresse, âge, etc.), que les données qui peuvent « *découler de*

[130] *Avec le RGPD, le groupe de l'article 29 de la Directive 95/46 (le « G29 »), qui était l'enceinte informelle d'échanges et d'élaboration de la doctrine, a été remplacé par le « Comité Européen de la Protection des Données » (le « CEPD »), institué par les articles 68 à 76 du RGPD.*

[131] *WP 242 rév.01, version révisée adoptée le 05/04/2017.*

l'observation de l'activité de cette dernière », telles que « *l'historique de recherche* », « *les données relatives au trafic* », « *les données de localisation d'une personne* » ou « *l'historique des transactions de la personne* »[132] ;

- lorsque les responsables de traitements traitent des informations qui contiennent des DCP de tiers, ces responsables de traitements « *ne devraient pas interpréter de manière trop restrictive l'expression « données à caractère personnel les concernant [relatives à la personne concernée]* ». En prenant l'exemple des registres des services de téléphonie qui incluent dans l'historique du compte de l'abonné les données de tiers concernés par des appels entrant ou sortant, le G29 précise que « *même si ces registres contiennent […] des données […] relatives à plusieurs personnes, les abonnés devraient pouvoir recevoir ceux-ci en réponse à leurs demandes de portabilité […] étant donné que ces registres se rapportent (également) à la personne concernée.* » ;

- s'agissant de l'atteinte aux droits et libertés des tiers, cette condition vise à empêcher l'extraction et la transmission de données contenant les DCP d'autres personnes concernées non consentantes. Néanmoins, le G29 précise, en prenant l'exemple du compte bancaire d'une personne, que, bien que ce dernier contienne des DCP relatives aux transactions d'autres personnes (par exemple en cas d'opérations de paiement au bénéficie du titulaire du compte), « *il est peu probable que les droits et libertés de ces tiers soient compromis par la transmission des informations concernant le compte bancaire du titulaire du compte dans le cadre d'une demande de portabilité, pour autant que, dans les deux exemples, les données soient utilisées à la même fin* ». Le G29 indique, à l'inverse, que « *les droits et libertés des tiers ne seront pas respectés si le nouveau responsable du traitement utilise les données à caractère personnel à d'autres fins, par exemple, si le responsable du traitement destinataire des données utilise les données d'autres personnes figurant dans le carnet d'adresse de la personne concernée à des fins de marketing* ».

Dans le cas des établissements assujettis, l'application de cette interprétation extensive du champ d'application du droit à la portabilité pourrait conduire les clients à exercer leur droit à la portabilité sur des relevés de compte intégrant des opérations de paiement (au crédit ou au débit) contenant des informations relatives à des tiers (bénéficiaires ou donneurs d'ordre) couvertes par le secret bancaire. Certaines de ces informations, dont l'établissement assujetti à eu connaissance dans l'exercice de son rôle de prestataire de services de paiement, peuvent, en effet, contenir des éléments précis et confidentiel relatives à ces tiers[133] qui bénéficient, comme rappelé précédemment (cf. *supra – section I/ B/ 2.*), de la protection du secret bancaire.

---

[132] *Le G29 précise toutefois que cette expression exclut les données résultant d'une analyse subséquente du comportement de la personne concernée et créées par le responsable de traitement (dans le cadre par exemple « d'un processus de personnalisation ou de recommandation, par catégorisation ou profilage des utilisateurs »).*

[133] *Au sein, notamment des zones libres (motifs et description du paiement) que les donneurs d'ordre doivent renseigner lorsqu'ils initient un virement bancaire.*

Si l'exercice du droit à la portabilité par un client qui demande communication de ses relevés de compte à lui-même ne pose pas difficultés en matière de secret bancaire (puisque les informations relatives à ces tiers lui ont été, *de facto*, communiquées par lesdits tiers à l'occasion des opérations passées sur le compte), il en va différemment lorsque le client exerce son droit à la portabilité en demandant à sa banque de communiquer ses relevés de compte directement à un autre responsable de traitement (Art. 20-2° RGPD). Dans ce cas en effet, les tiers seraient en droit de se prévaloir du secret bancaire qui protège leurs informations et il apparaît complexe pour la banque d'apprécier, de son propre chef, si ce droit au secret pourrait être compromis par cette communication d'informations à un responsable de traitement tiers.

Nonobstant les Lignes Directrices du G29, et afin de mettre l'établissement assujetti à l'abri des poursuites pénales pour violation du secret bancaire, l**e groupe de travail estime ainsi, lorsque le droit à la portabilité est exercé par un client sur ses relevés et qu'il demande leur transmission directement à un autre responsable de traitement, que le secret bancaire est de nature à justifier d'exciper ces relevés de ce droit à la portabilité**. En effet :

- le RGPD n'exclut pas l'application des dispositions du droit interne des États membres, en ce compris les dispositions encadrant le secret professionnel ;

- il apparaît matériellement impossible, lorsqu'un client exerce son droit à la portabilité sur ses relevés de compte (ou toute autre donnée de paiement) contenant des informations relatives à des tiers, de recueillir auprès de ces derniers un consentement exprès pour lever le secret au profit du responsable de traitements destinataire ;

- le secret bancaire est un droit dont bénéficient ces tiers et le RGPD précise explicitement, et sans distinguer, que le droit à la portabilité « *ne porte pas atteinte aux droits et libertés de tiers* » ;

- tout comme pour la communication du verso d'un chèque et la difficile articulation entre secret bancaire et droit de la preuve (cf. *supra – section II/*), l'établissement assujetti sera rarement en mesure d'apprécier lui-même lequel des deux droits fondamentaux qui s'opposent dans cette problématique doit l'emporter : le droit à la portabilité du demandeur d'une part, le droit au secret bancaire du tiers d'autre part. Cette appréciation relève du contrôle souverain des juges du fond (et doit le rester).

Une modification de la loi visant à créer une nouvelle exception au secret bancaire dans cette hypothèse n'est pas apparue opportune au groupe de travail dans la mesure où il s'agirait d'une exception particulièrement large et touchant au droit dont bénéficient des tiers à la demande de portabilité. **Afin de pouvoir concilier le droit à la portabilité des clients des établissements assujettis d'une part, et le respect du droit des tiers (ie. le droit au secret dont ils bénéficient) d'autre part, il est à l'inverse préconisé que la doctrine de la CNIL en la matière soit revue à la lumière de cette problématique (cf. *Recommandation n° 13*).**

5.1.2 - Consentement aux traitements de données à caractère personnel et secret bancaire

Tout traitement de DCP nécessite d'être fondé sur l'une des six bases juridiques offertes par l'article 6-1 du RGPD, notamment : l'exécution d'un contrat, l'exécution d'une obligation légale, la poursuite des intérêts légitimes du responsable de traitements, le consentement de la personne concernée.

Le « consentement », comme base juridique d'un traitement de DCP, n'est, en pratique, retenu que lorsqu'aucune des cinq autres bases juridiques n'est pertinente ou lorsqu'une disposition légale ou réglementaire l'impose[134].

Pour que le consentement de la personne soit valablement recueilli et que le traitement sur lequel il se fonde puisse être mis en œuvre de façon licite, celui-ci doit répondre à la définition donnée par l'article 7 du RGPD. Cet article dispose que le consentement doit être spécifique[135] (ie. dissocié des autres questions qui seraient posées à la personne au même moment), posé sous une forme compréhensible et donné librement[136].

Sur le critère de l'expression d'un consentement libre, l'article 7-4 du RGPD dispose également que pour « *déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données […] qui n'est pas nécessaire à l'exécution dudit contrat* ». Cet alinéa doit se comprendre en ce sens que le consentement qui serait éventuellement requis au titre d'un traitement de DCP ne doit pas subordonner l'exécution d'un contrat ou d'un service sauf lorsque l'absence de mise en œuvre dudit traitement rend effectivement impossible la fourniture du service ou l'exécution du contrat par le responsable du traitement. Dans ce cas en effet, le traitement trouverait son fondement juridique, non pas dans le consentement, mais, *a fortiori*, dans l'exécution du contrat.

Cette interprétation a été confirmée par le G29 dans ses Lignes Directrices sur le consentement au sens du RGPD[137]. Il rappelle en préambule que « *le consentement ne peut constituer une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation et le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice* ». Le G29 considère que, s'agissant de la manifestation de la volonté libre, le consentement n'est pas valablement donné lorsqu'il est présenté « *comme une partie non négociable des conditions générales* ».

---

[134] *C'est le cas notamment pour les traitements de DCP ayant pour finalité la prospection commerciale par voie électronique (articles L.34-5 du Code des postes et des communications électroniques et L.223-7 du Code de la consommation) ou lorsqu'un traitement ultérieur est envisagé et que sa finalité est incompatible avec la finalité initiale pour laquelle les DCP ont été collectées (conformément aux dispositions de l'article 6-4 du RGPD).*

[135] *Article 7-2 du RGPD.*

[136] *Article 7-2 du RGPD.*

[137] *WP259 rév.01, version révisée et adoptée le 10 avril 2018.*

Le groupe de travail s'est, dans ces conditions, interrogé sur l'articulation entre cette notion de « consentement », en tant que base juridique d'un traitement de DCP, et la notion de consentement telle qu'elle est traditionnellement appliquée en droit français.

Se confondent-elles ? Se juxtaposent-elles ? Si le présent rapport n'apporte pas de réponse à cette question, une illustration de cette articulation complexe peut néanmoins être développée : la transmission de DCP à des tiers dans le cadre d'une modification de la convention de compte de dépôt à vue.

Les établissements assujettis peuvent être amenés à mettre en place des traitements de DCP nécessitant une transmission à des tiers (sous-traitants par exemple) qui trouvent leur base juridique dans le consentement des personnes[138] et qui, par ailleurs, nécessitent une levée du secret bancaire au profit des récipiendaires de ces DCP.

Il est d'usage que les établissements de crédit insèrent au sein des conventions de compte les liant à leurs clients une clause « Secret professionnel » listant, précisément, les situations dans lesquelles le client délie l'établissement de son obligation de secret[139]. La mise en place d'un tel traitement de DCP peut donc nécessiter de modifier cette clause de la convention de compte par application de la procédure légale de l'article L.312-1-1 du Code monétaire et financier pour introduire cette nouvelle situation.

Cette procédure organise une modalité particulière de recueil du consentement des clients lorsqu'un établissement de crédit modifie les dispositions de la convention de compte qui les lie à eux. L'article L.312-1-1 du Code monétaire et financier dispose ainsi que : « *Tout projet de modification de la convention de compte de dépôt est fourni sur support papier ou sur un autre support durable au client au plus tard deux mois avant la date d'application envisagée. Selon les modalités prévues dans la convention de compte de dépôt, l'établissement de crédit informe le client qu'il est réputé avoir accepté la modification s'il ne lui a pas notifié, avant la date d'entrée en vigueur proposée de cette modification, qu'il ne l'acceptait pas ; dans ce cas, l'établissement de crédit précise également que, si le client refuse la modification proposée, il peut résilier la convention de compte de dépôt sans frais, avant la date d'entrée en vigueur proposée de la modification* ». Cette procédure permet ainsi aux établissements de recueillir le consentement de son client sur les modifications d'une convention de compte sauf opposition de leur part et à la condition de les lui avoir notifier deux mois avant leur entrée en vigueur.

---

[138] *Notamment lorsque ces traitements ne trouvent leur fondement juridique ni dans l'exécution de la convention de compte, ni dans l'intérêt légitime de la banque, responsable de traitement.*

[139] *En ce sens, voir section I/, D/, 1. du rapport.*

Il est apparu au groupe de travail que la sollicitation de deux consentements distincts (un consentement au titre de la base juridique du traitement de DCP et un consentement au titre de la modification de la convention de compte) ayant pratiquement le même objet serait difficilement compréhensible par les clients. Aussi, il a considéré que, au regard notamment de la volumétrie très importante de clients concernés, le recueil du consentement des clients par application de la procédure légale prescrite par l'article L.312-1-1 précité pour modifier la clause « Secret professionnel » de la convention de compte (et leur rendre opposable) peut valoir recueil du consentement au titre du traitement de DCP sous-jacent à cette modification contractuelle[140].

5.2 - Secret bancaire et service d'information sur les comptes

L'un des apports majeurs de la Directive 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, dite Directive Service de Paiement II ou « DSP2 »[141], a été de consacrer dans les textes et de réglementer l'activité de nouveaux acteurs de paiement, en particulier les prestataires fournissant le service d'information sur les comptes (communément appelé, service « d'agrégation »)[142].

Le service d'information sur les comptes, introduit dans la liste des services de paiement de l'article L.314-1 du Code monétaire et financier, est défini au 7° de l'article D.314-2 du même code comme « *un service en ligne consistant à fournir des informations consolidées concernant un ou plusieurs comptes de paiement détenus par l'utilisateur de services de paiement soit auprès d'un autre prestataire de services de paiement, soit auprès de plus d'un prestataire de services de paiement.* »

De façon concrète, il consiste, pour le prestataire fournissant ce service[143] (ci-après le « PSIC »), à restituer à son utilisateur les informations relatives aux comptes de paiement (identification, solde, opérations de paiement passées sur ledit compte, etc.) qu'il détient dans les livres d'un autre établissement : l'établissement teneur du compte. La restitution de ces informations à l'utilisateur final nécessite donc pour le PSIC d'y accéder au préalable directement au sein du système informatique de l'établissement teneur de compte.

---

[140] Étant précisé que l'établissement pourrait, dans ces conditions, offrir aux clients, en complément, la possibilité de s'opposer à la mise en place dudit traitement de DCP sans pour autant que cela n'entraîne résiliation de sa convention de compte (comme le prévoit la dernière disposition de l'article L.312-1-1 du Code monétaire et financier).

[141] La DSP2 a été transposée dans le Code monétaire et financier par l'ordonnance n° 2017-1252 du 9 août 2017 et est entrée en vigueur le 13/01/2018.

[142] La DSP2 a également introduit dans la réglementation le service d'initiation de paiement défini au 6° de l'article D.314-2 du Code monétaire et financier.

[143] Le service d'information sur les comptes peut être fourni par les établissements de crédit et les établissements de paiement, ainsi que par une nouvelle catégorie de prestataires de services de paiement (« PSP ») créée par la DPS2 : les prestataires de services d'information sur les comptes. L'article L.522-1 II du Code monétaire et financier définit cette nouvelle catégorie de PSP comme toute personne physique ou morale, autre que les établissements de crédit et les établissement de paiement, qui fournit à titre de profession habituelle le service d'information sur les comptes à l'exclusion de tout autre service de paiement.

Si les textes de transposition de la DSP2 ont bien prévu l'assujettissement des PSIC au secret professionnel[144], ils n'ont en revanche introduit aucune exception légale venant, spécifiquement, délier l'établissement teneur du compte du secret professionnel auquel il est tenu sur les informations de son propre client à l'égard du PSIC.

Même en l'absence de dispositions légales spécifiques, on peut néanmoins considérer que l'ensemble des nouvelles dispositions du Code monétaire et financier encadrant la fourniture du service d'information sur les comptes constitue *de facto* une situation de « secret partagé » permettant ainsi aux établissements gestionnaires des comptes de paiement de communiquer avec le PSIC sans avoir à obtenir, au préalable, le consentement exprès de leur client à cette fin.

Cette analyse se déduit des dispositions de l'article L.133-41 du Code monétaire et financier qui liste les conditions de mise en œuvre du service d'information sur les comptes et qui prévoit un mandat confié par l'utilisateur du service en vertu duquel le PSIC peut fournir le service :

- l'utilisateur accède « *aux données de ses comptes de paiement* ***par l'intermédiaire*** *d'un prestataire de services de paiement de son choix fournissant le service d'information sur les comptes* »[145] ;

- le PSIC doit **recueillir le consentement exprès** de l'utilisateur[146] ;

- le PSIC ne peut accéder et restituer que les « ***informations provenant des comptes de paiement désignés par l'utilisateur*** *de services de paiement et des opérations de paiement associées* »[147] ;

Les dispositions légales prévoient par ailleurs que le PSIC « *s'identifie, pour chaque session de communication, auprès du ou des prestataires de paiement gestionnaires de comptes de l'utilisateur […] et communique de manière sécurisé* »[148] conformément aux dispositions de l'acte délégué portant Normes Techniques de Règlementation (« RTS ») adopté par l'ABE le 14 mars 2018 et qui s'appliquent depuis le 14 septembre 2019.

Du fait de ces modalités d'authentification (du PSIC, mais également de l'utilisateur) auprès de l'établissement gestionnaire des comptes, ce dernier dispose ainsi de la certitude que l'accès aux comptes a expressément été demandé par son client en vertu du mandat qu'il a confié au PSIC et,

---

[144] *Conformément aux articles L.511-33 et L.522-19 du Code monétaire et financier pour, respectivement, les établissements de crédit et les établissement de paiement. Les prestataires de services d'information sur les comptes sont quant à eux traités comme des établissements de paiement pour l'application de l'article L522-19 du Code monétaire et financier en vertu de l'article L.522-11-2 II, 4e alinéa, du même code.*

[145] *Article L.133-41 I du Code monétaire et financier.*

[146] *Article L.133-41 II 1° du Code monétaire et financier.*

[147] *Article L.133-41 II 4° du Code monétaire et financier.*

[148] *Article L.133-41 II 3° du Code monétaire et financier.*

au final, que cet utilisateur a bien expressément accepté de partager le secret bancaire pesant sur ces informations avec le PSIC. Dans ces conditions, il n'apparaît pas nécessaire que l'établissement gestionnaire des comptes recueille, par ailleurs et au préalable, une autorisation expresse pour lever le secret bancaire vis-à-vis de tout PSIC auquel son client pourrait recourir[149].

Si la question ne laisse ainsi pas de doutes s'agissant des informations couvertes par le périmètre du service d'information sur les comptes tel qu'il est réglementé par le Code monétaire et financier, l'absence de dispositions légales spécifiques demeure néanmoins source d'insécurité juridique dans deux situations particulières :

(i) « L'agrégation » est un service qui existait avant la DSP2 et qui, dans la pratique, ne se limite pas à restituer les seules informations des comptes de paiement détenus par leurs utilisateurs.

De façon beaucoup plus large, les entreprises qui fournissent un service d'agrégation proposent en règle générale une consolidation des informations de l'ensemble des avoirs, produits et services détenus par les utilisateurs dans les livres des établissements gestionnaires (produits d'épargne, titres financiers, crédits, etc.). Depuis l'entrée en vigueur des dispositions issues de la DSP2, ces services d'agrégation continuent à être délivrés sur ce périmètre plus large que les simples comptes de paiement.

Dans ce contexte, et alors que les obligations pesant sur les PSIC ne s'appliquent qu'à la fourniture des informations « *concernant un ou plusieurs comptes de paiement*[150] » (notamment l'obligation d'obtenir un mandat spécial de l'utilisateur et de communiquer avec les établissements gestionnaires de comptes dans les conditions fixées par les RTS), le groupe de travail s'est interrogé sur le fait de savoir si les établissements teneurs des comptes peuvent raisonnablement considérer que le secret bancaire est également levé sur les informations qui dépassent les comptes de paiement de l'utilisateur. En effet, le groupe de travail a constaté que les établissements teneurs de comptes n'ont pas accès au mandat donné par leurs clients au PSIC et ne peuvent, *de facto*, ainsi pas vérifier, dans les faits, le contenu et la portée de ce mandat.

---

[149] Si l'établissement gestionnaire des comptes n'obtenait pas cette autorisation expresse, cela pourrait, au demeurant, être susceptible de placer l'établissement gestionnaire des comptes de paiement en infraction aux dispositions de l'article L.133-41 III 1° du Code monétaire et financier qui prévoient que l'établissement gestionnaire du compte doit traiter « les demandes de données transmises par le PSP fournissant le service d'information sur les comptes sans aucune discrimination, autre que fondée sur des raisons objectives ».

[150] Sont des comptes de paiement, les comptes détenus au nom d'un ou de plusieurs utilisateurs de services de paiement et qui sont utilisés aux fins de l'exécution d'opérations de paiement (Articles 4 12 de la DSP2 / Articles L.314-1 et L.522-4 du Code monétaire et financier) : les comptes de dépôt à vue et les comptes ouverts par les établissements de paiement sont des comptes de paiement. En revanche, les comptes d'épargne (ou de titres) ne relèvent pas de cette catégorie puisqu'ils n'ont pas pour finalité d'exécuter des opérations de paiement quotidiennes. Il est à noter que certains types de compte d'épargne, tel que le livret A, peuvent toutefois permettre de façon accessoire et limitative, l'exécution d'opération de paiement sans pour autant recevoir la qualification de compte de paiement au sens du Code monétaire et financier puisque leur finalité n'est pas, exclusivement, l'exécution d'opérations de paiement (Revue Banque n°788 du 13/10/2015 : « Brèves remarques sur le compte de paiement », Pierre Storrer, Avocat au Barreau de Paris, Kramer Levin Naftalis & Frankel LLP).

(ii) Avant que les entreprises fournissant un service d'information sur les comptes n'aient vu leur activité régulée, ces derniers utilisaient la technique du *web-scraping*.

Cette technique permet de récupérer, par l'usage des données de sécurité personnalisées du client (identifiant et code personnel d'accès aux espaces de banque en ligne), le contenu d'une page Internet afin d'en réutiliser le contenu et se faisant, d'accéder à toutes les données accessibles sur le portail de banque en ligne des clients. La particularité de cette technique réside dans le fait qu'elle permet d'accéder à l'ensemble des données bancaires du client présentes sur son espace personnel de banque en ligne, bien au-delà des simples informations relatives aux comptes de paiement pour lesquelles les PSIC disposent du mandat prévu par l'article L.133-41 du Code monétaire et financier.

Or, si les RTS sont venues encadrer les modalités de communication entre les PSIC et les établissements gestionnaires de compte, elles n'ont pas interdit l'usage de la technique du *web-scraping* (pour autant que les PSIC respectent l'ensemble des conditions fixées par lesdits RTS)[151]. De surcroît, pour les entreprises proposant un service d'agrégation allant au-delà du service réglementé par la DPS2, la technique du *web-scraping* reste largement employée.

Si l'analyse développée précédemment permet d'avoir l'assurance que le secret bancaire est levé sur les informations incluses dans le mandat spécial donné par l'utilisateur au PSIC (comptes de paiement et données des opérations de paiement associées), le groupe de travail estime, à l'inverse, qu'elle pourrait souffrir la contestation pour les autres informations non incluses dans ce mandat auxquelles le PSIC a accès *via* à la technique du *web-scraping*[152].

Le groupe de travail a considéré que la problématique du service d'informations sur les comptes, et notamment celle de son périmètre (compte de paiement vs. autres types de comptes ou de produits bancaires) et des technologies utilisées (*webscrapping*), dépassait le strict cadre du secret bancaire et **a ainsi estimé que ces questions devaient être traitées de façon plus globale par les pouvoirs publics et les acteurs concernés au niveau européen.**

[151] Les établissements français ont opté, pour le service d'information sur les comptes réglementé (ie. sur le strict périmètre des comptes de paiement), pour une communication basée, en lieu et place du web-scraping, sur des interfaces de programmation applicative (ou Application Programming Interface - « API ») ne nécessitant plus la communication au PSIC des données de sécurité personnalisées de l'utilisateur et limitant l'accès aux seules informations des comptes de paiement désignés par l'utilisateur.

[152] Il convient néanmoins de noter que les services d'agrégation sont fournis depuis de nombreuses années au moyen de cette technique et qu'aucune sanction ou décision de jurisprudence sur le terrain de la violation du secret professionnel n'a été identifiée dans ce contexte particulier.

5.3 - Secret bancaire et loi étrangère à portée extraterritoriale : l'exemple du *Cloud Act*

Le secret bancaire est parfois confronté à des textes de portées extraterritoriales, pouvant avoir pour objet direct ou effet induit de rendre l'application de ce dernier complexe, voire impossible. L'un de ces textes, le *Clarifying Lawful Overseas Use of Data Act* (plus communément appelé *Cloud Act*) mérite une attention toute particulière, dans la mesure où les autorités américaines entendent faire de cette loi le standard international en matière de production de preuves en matière pénale.

L'examen de ce texte, et de son incompatibilité avec les principes du secret bancaire, ne donne pas lieu à une préconisation d'évolution de textes au sein du présent rapport, ces textes étant actuellement en gestation au niveau européen. En revanche, il est l'occasion de souligner la nécessaire vigilance des pouvoirs publics à propos de procédures remettant directement en cause, entre autres principes, celui du secret bancaire. Le groupe de travail a ainsi estimé utile d'insérer en *Annexe n° 3* au présent rapport une note d'analyse dédiée au *Cloud Act* et aux problématiques qu'il soulève en matière de secret bancaire.

VI- Recommandations du groupe de travail

Référence du rapport	Recommandation
Recommandation n° 1	
Chapitre I, H/ **Pages 27-28**	Compte tenu de ce foisonnement d'exceptions au sein de multiples textes, le groupe de travail a estimé qu'il serait souhaitable de procéder à une rationalisation des textes en vigueur en rassemblant, au sein d'un corpus unique et cohérent, l'ensemble des dérogations au secret bancaire et en apportant les précisions textuelles nécessaires à la détermination des informations couvertes par le secret. Il est ainsi préconisé qu'un travail doctrinal réunisse l'ensemble des exceptions au secret bancaire, la création d'un ouvrage par la Doctrine lui apparaissant plus approprié qu'une réforme législative, eu égard à la multitude de textes et de régimes applicables.
Recommandation n° 2	
Chapitre II, C/ **Page 38**	Il conviendrait d'ajouter à l'article L.511-33 du Code monétaire et financier un alinéa complémentaire afin de couvrir l'hypothèse d'une levée du secret en cas de procédure judiciaire entre l'établissement assujetti et son client. Cet alinéa pourrait être rédigé de la façon suivante : « *Les établissements de crédit et les sociétés de financement peuvent, dans le cadre des procédures judiciaires qu'ils ont initiées contre leurs clients ou initiées par ces derniers à leur encontre, communiquer des informations couvertes par le secret professionnel concernant ces clients, sous réserve que la production de ces informations soit nécessaire au succès de leurs prétentions.* »
Recommandation n° 3	
Chapitre II, C/ **Page 39**	Un dispositif similaire, prévu par les articles L.153-1 et 153-2 du Code de commerce, existe déjà en matière de secret des affaires ; il pourrait être adapté au secret bancaire. Il pourrait être inséré dans le code monétaire et financiers un article L.511-33-1 rédigé en les termes suivants : « *Lorsque, à l'occasion d'une instance civile ou commerciale ayant pour objet une mesure d'instruction sollicitée avant tout procès au fond ou à l'occasion d'une instance au fond, il est fait état ou est demandé, en dehors des cas de levée du secret bancaire prévus par l'article L.511-33, la communication ou la production d'une pièce dont il est allégué par une partie ou un tiers ou dont il a été jugé qu'elle est de nature à porter atteinte au secret bancaire, les parties peuvent saisir le juge afin qu'il autorise sa production. Le juge autorise la production de la pièce comportant des éléments couverts par le secret bancaire lorsque celle-ci est indispensable à l'exercice du droit à la preuve et proportionnée aux intérêts antinomiques en présence.* *Afin de limiter l'atteinte au secret professionnel prévu par l'article L.511-33, le juge peut, d'office ou à la demande d'une partie ou d'un tiers :*

Référence du rapport	Recommandation
	1° prendre connaissance seul de cette pièce et, s'il l'estime nécessaire, ordonner une expertise et solliciter l'avis, pour chacune des parties, d'une personne habilitée à l'assister ou la représenter, afin de décider s'il y a lieu d'appliquer des mesures de protection prévues au présent article ; *2° décider de limiter la communication ou la production de cette pièce à certains de ses éléments, en ordonner la communication ou la production sous une forme de résumé ou en restreindre l'accès, pour chacune des parties, au plus à une personne physique et une personne habilitée à l'assister ou la représenter ;* *3° décider que les débats auront lieu et que la décision sera prononcée en chambre du conseil ;* *4° adapter la motivation de sa décision et les modalités de publicité de celle-ci aux nécessités de la protection du secret bancaire.* »
Recommandation n° 4	
Chapitre III, A/ **Page 40**	Le champ de la sous-traitance bancaire dépassant largement le seul cadre des activités essentielles externalisées (par exemple la, sous-traitance des fonctions juridiques, comptables, la facturation, les ressources humaines, ou encore les achats de prestations standard, etc.), il est recommandé de supprimer la notion de « *fonctions opérationnelles importantes* » de l'article L.511-33, 3e alinéa, 6°, du Code monétaire et financier.
Recommandation n° 5	
Chapitre III, B/, 1. **Pages 42-43**	Afin de lever toute ambiguïté et de clarifier sans aucun doute possible que, lors des contrôles de l'AFA portant sur un établissement assujetti, le secret bancaire ne peut lui être opposé, il est proposé une clarification des textes par le biais d'une modification ciblée de l'article L.511-33 du Code monétaire et financier qui serait de nature à permettre une communication des éléments demandés relevant du secret bancaire. L'article L. 511-33 pourrait être modifié de la manière suivante (proposition de modification en gras) : « *Tout membre d'un conseil d'administration et, selon le cas, d'un conseil de surveillance et toute personne qui à un titre quelconque participe à la direction ou à la gestion d'un établissement de crédit ou d'un organisme mentionné au 5 de l'article L. 511-6 ou qui est employée par l'un de ceux-ci est tenu au secret professionnel.* *Outre les cas où la loi le prévoit, le secret professionnel ne peut être opposé ni à l'Autorité de contrôle prudentiel ni à la Banque de France ni à l'autorité judiciaire agissant dans le cadre d'une procédure pénale* ***ni à l'Agence française anticorruption****. […]* »
Recommandation n° 6	
Chapitre III, B/, 2. **Pages 43**	Il est souhaité que les banques n'appartenant pas au même groupe puissent avoir la possibilité de s'échanger des informations pour les besoins de la surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme lorsqu'elles sont désignées dans le cadre du droit au compte par la Banque de France. Cela

Référence du rapport	Recommandation
	permettrait à la banque désignée de mettre en place une vigilance appropriée dans les meilleurs délais. L'article L.561-21 du Code monétaire et financier pourrait ainsi être modifié comme suit (proposition de modification en gras) : *« **I.-** Par dérogation à l'article L. 561-18, les personnes mentionnées aux 1° à 7° quater et aux 12°, 12° bis, 13°, 18° et 19° de l'article L. 561-2 peuvent, lorsqu'elles interviennent pour un même client et dans une même opération ou lorsqu'elles ont connaissance, pour un même client, d'une même opération, s'informer mutuellement, et par tout moyen sécurisé, de l'existence et du contenu de la déclaration prévue à l'article L. 561-15. Ces échanges d'informations ne sont autorisés, parmi les personnes énumérées à l'article L. 561-2, qu'entre celles mentionnées aux 1° à 7° ou entre celles mentionnées aux 1° bis, 1° ter et 1° quater qui fournissent principalement le service mentionné au 6° du II de l'article L. 314-1, ou entre celles mentionnées aux 7° bis à 7° quater. Ils sont également autorisés entre les personnes mentionnées aux 12°, 12° bis, 13° à 19° du même article L. 561-2 ou entre celles mentionnées à son 18° et les avocats mentionnés au 13°, si les conditions suivantes sont réunies :* *a) les personnes mentionnées aux 1° à 7° quater et aux 12°, 12° bis, 13°, 18° et 19° de l'article L. 561-2 sont situées en France, dans un Etat membre de l'Union européenne ou partie à l'accord sur l'Espace économique européen ;* *b) lorsque l'échange d'informations implique des personnes qui ne sont pas situées en France, celles-ci sont soumises à des obligations équivalentes en matière de secret professionnel ;* *c) les informations échangées sont utilisées exclusivement à des fins de prévention du blanchiment des capitaux et du financement du terrorisme ;* *d) le traitement des informations communiquées, lorsqu'il est réalisé dans un pays tiers, garantit un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes, conformément aux articles 122 et 123 de la loi n° 78-17 du 6 janvier 1978 mentionnée ci-dessus.* ***II.- Les personnes mentionnées aux 1° de l'article L. 561-2 peuvent également s'informer mutuellement, par tout moyen sécurisé, des motifs de clôture d'un compte lorsqu'elles sont désignées au titre du III de l'article L.312-1.*** ***III. Les informations échangées dans le cadre du I et du II sont utilisées exclusivement à des fins de prévention du blanchiment des capitaux et du financement du terrorisme.*** »
Recommandation n° 7	
Chapitre III, C/, 1. **Page 44-45**	La loi pourrait prévoir que les établissements assujettis pourront communiquer des informations de contact des clients dont ils disposent, couvertes par le secret professionnel, aux distributeurs, dans le cadre d'un rappel de produits, si ces derniers confirment qu'elles sont

Référence du rapport	Recommandation
	nécessaires à la sauvegarde des intérêts vitaux de la personne concernée (l'utilisateur de services de paiement) ou d'une autre personne physique (ses proches). Une définition très large de l'intérêt vital serait dans ces conditions nécessaire. Une définition de la sauvegarde des intérêts vitaux conforme à l'avis de 2014 pourrait être prévue dans les textes. Cette définition sera applicable spécifiquement à cette nouvelle dérogation au secret bancaire et il faudra la distinguer de la notion voisine issue du RGPD.
Recommandation n° 8	
Chapitre III, C/, 2. **Page 48-49**	S'agissant ici d'appliquer un principe général de droit pénal qui n'est pas spécifique à la matière bancaire et financière et qui, à la connaissance du groupe de travail, n'a pas donné lieu à des décisions judiciaires publiées le mettant en œuvre dans un tel contexte, ses contours sont toujours évidemment difficiles à appréhender avec certitude. Dans ce contexte, le rapport préconise que l'analyse qui y est développée *supra* soit confirmée par une circulaire du Ministère de la Justice.
Recommandation n° 9	
Chapitre IV, A/ **Page 51-52**	Les alinéas 3 et 6 de l'article L.511-33-I du Code monétaire et financier pourraient être modifiés comme suit (proposition de modification en gras) : « *Les établissements de crédit et les sociétés de financement peuvent par ailleurs communiquer des informations couvertes par le secret professionnel, d'une part, aux agences de notation pour les besoins de la notation des produits financiers et, d'autre part, aux personnes,* ***ou à celles qui leurs sont substituées****, avec lesquelles,* ***ou par l'intermédiaire desquelles****, ils* ***étudient, élaborent,*** *négocient, concluent ou exécutent les opérations ci-après énoncées,* ***ainsi qu'à toute personne leur fournissant une prestation d'assistance ou de conseil financier, comptable, juridique ou technique****, dès lors que ces informations sont nécessaires à celles-ci.* » « *Les personnes recevant des informations couvertes par le secret professionnel, qui leur ont été fournies pour les besoins d'une des opérations ci-dessus énoncées, doivent les conserver confidentielles****~~, que l'opération susvisée aboutisse ou non. Toutefois, dans l'hypothèse où l'opération susvisée aboutit, ces.~~*** ***Ces*** *personnes peuvent à leur tour communiquer les informations couvertes par le secret professionnel,* ***d'une part, à leurs conseils, mandataires, fournisseurs ou sous-traitants sous réserve qu'ils s'engagent contractuellement à en conserver la confidentialité et, d'autre part,*** *dans les mêmes conditions que celles visées au présent article aux personnes,* ***ou à celles qui leurs sont substituées,*** *avec lesquelles,* ***ou par l'intermédiaire desquelles****, elles* ***étudient, élaborent,*** *négocient, concluent ou exécutent les opérations énoncées ci-dessus* ***ainsi qu'à toute personne leur fournissant une prestation d'assistance ou de conseil financier, comptable, juridique ou technique et à leurs propres conseils,***

Référence du rapport	Recommandation
	mandataires, fournisseurs ou sous-traitants sous réserve qu'ils s'engagent contractuellement à en conserver la confidentialité. »
Recommandation n° 10-a	
Chapitre IV, B/, 1 **Page 53**	Le paragraphe 1° de l'alinéa 3 de l'article L. 511-33-I du Code monétaire et financier pourrait être modifié comme suit (proposition de modification en gras) : « *1° Opérations de crédit* ***~~effectuées, directement ou indirectement, par un ou plusieurs établissements de crédit ou sociétés de financement~~*** *;* »
Recommandation n° 10-b	
Chapitre IV, B/, 2 **Page 54**	Le paragraphe 2° de l'alinéa 3 de l'article L. 511-33-I du Code monétaire et financier pourrait être modifié comme suit (proposition de modification en gras) : « *2° Opérations* ***~~sur instruments financiers, de garanties ou d'assurance~~*** *destinées à la couverture* ***ou à la gestion ~~d'un risque de crédit~~ de tous risques auquel ils sont exposés*** *;* »
Recommandation n° 10-c	
Chapitre IV, B/, 3 **Page 54**	Le paragraphe 7° de l'alinéa 3 de l'article L. 511-33-I du code monétaire et financier pourrait être modifié comme suit (proposition de modification en gras) : « *7°* ***~~Lors de l'étude ou l'élaboration de tout type de~~*** *Tous contrats ou ~~d'~~opérations, dès lors que ces* ***~~entités~~*** *personnes appartiennent au même groupe que l'auteur de la communication.* »
Recommandation n° 10-d	
Chapitre IV, B/, 4 **Page 55**	Un nouveau paragraphe 8°, rédigé comme suit, pourrait être ajouté à l'alinéa 3 de l'article L. 511-33-I du Code monétaire et financier : « *8° Toute opération de banque, de paiement, de monnaie électronique ou toute autre opération, effectuée pour les besoins de la fourniture des services à la clientèle.* »
Recommandation n° 10-e	
Chapitre IV, B/, 5 **Page 55**	Un nouvel alinéa 5, rédigé comme suit, pourrait être inséré entre les actuels 4e et 5e alinéa de l'article L. 511-33-I du Code monétaire et financier : « *Lors d'opérations de titrisation, les établissements de crédit et les sociétés de financement peuvent également communiquer, notamment aux investisseurs, des informations couvertes par le secret professionnel dans le cadre du règlement (UE) 2017/2402 du parlement européen et du conseil du 12 décembre 2017 créant un cadre général pour la titrisation ainsi qu'un cadre spécifique pour les titrisations simples, transparentes et standardisées, ou dans le cadre de toute*

Référence du rapport	Recommandation
	législation ou réglementation équivalente d'un État qui n'est pas membre de l'Union européenne. »
Recommandation n° 11	
Chapitre IV, C/ Page 57	L'ajout au 3e et 6e alinéas de l'article L.511-33-I du Code monétaire et financier d'une mention spécifique aux personnes « *par l'intermédiaire desquelles* » certaines opérations sont négociées, conclues ou exécutées « *ainsi qu'à toute personne leur fournissant une prestation d'assistance ou de conseil financier, comptable, juridique ou technique* » en conjonction avec les modifications proposées par ailleurs aux termes de la Recommandation n° 9 permettraient de répondre à cette préoccupation.
Recommandation n° 12	
Chapitre IV, D/ Page 59	Dans une logique de protection de la clientèle et de traitement équitable des différents acteurs réglementés, les prestataires de services sur actifs numériques (PSAN) et les plateformes de crowdfunding (intermédiaires en financement participatif / conseillers en investissement participatif) devraient être soumis au secret professionnel.
Recommandation n° 13	
Chapitre V, A/, 1. Page 63	Une modification de la loi visant à créer une nouvelle exception au secret bancaire dans cette hypothèse n'est pas apparue opportune au groupe de travail dans la mesure où il s'agirait d'une exception particulièrement large et touchant au droit dont bénéficient des tiers à la demande de portabilité. Afin de pouvoir concilier le droit à la portabilité des clients des établissements assujettis d'une part, et le respect du droit des tiers (ie. le droit au secret dont ils bénéficient) d'autre part, il est à l'inverse préconisé que la doctrine de la CNIL en la matière soit revue à la lumière de cette problématique.

ANNEXE 1

Composition du groupe de travail

COMPOSITION DU GROUPE DE TRAVAIL
« Secret bancaire »

PRÉSIDENT :

- **Pierre MINOR,** Directeur Juridique, Groupe Crédit Agricole, membre du Haut Comité Juridique de la Place Financière de Paris (HCJP)

MEMBRES :

- **Christophe ARNAUD,** Directeur des Services Juridiques, Banque de France
- **Emilie BAILLY,** spécialiste juridique, Autorité de Contrôle Prudentiel et de Résolution (ACPR)
- **Claire BOIGET,** Directrice Juridique, Association Française des Marchés Financiers (AMAFI)
- **Alban CAILLEMER du FERRAGE,** Avocat associé Jones Day, Professeur des Universités, associé à l'Université Paris 2 Panthéon-Assas, membre du HCJP
- **Côme CHOMBART de LAUWE,** Chargé de mission, Fédération Bancaire Française (FBF)
- **Christophe DE BEER,** Deputy Head of Banking, Financing & Securitisation, Legal, Crédit Agricole CIB
- **Nadège DEBENEY,** Avocat, Jones Day
- **Hubert de VAUPLANE,** Avocat associé, Kramer Levin Naftalis & Frankel LLP, membre du HCJP
- **Romain DUCATEZ,** Juriste référent Pôle Bancaire et Moyens de Paiement, Direction Juridique Groupe, Groupe BPCE
- **Pénélope DUTET,** Directrice du Département Juridique, Agence Française de Développement (AFD)
- **Gérard GARDELLA,** ancien Magistrat, ancien Directeur Juridique du groupe Société Générale, Secrétaire Général du HCJP
- **Étienne GASTEBLED,** Avocat associé, Lussan
- **Pauline HOTTIN JOLY,** Doctorante au HCJP
- **Sophie HERVIER,** spécialiste juridique, ACPR
- **Emmanuel JOUFFIN,** Responsable du département veille réglementaire groupe, La Banque Postale
- **Léa KARAGEUZIAN,** Juriste, bureau du droit des sociétés et de l'audit, Direction des Affaires Civiles et du Sceau, Ministère de la Justice

- **Frédéric LACROIX,** Avocat associé, Clifford Chance Europe LLP, membre du HCJP
- **Arnaud LEMEUX,** Chef du Service Droit Bancaire et Missions d'Intérêt Général, Direction des Services Juridiques, Banque de France
- **Flavie le TALLEC,** Magistrate, Chef du bureau du droit des sociétés et de l'audit, Direction des Affaires Civiles et du Sceau, Ministère de la Justice
- **Alice NAVARRO,** Magistrate, Conseillère juridique, Direction Générale du Trésor
- **Françoise PALLE-GUILLABERT,** Déléguée générale de l'Association française des Sociétés Financières (ASF)
- **Jérôme PEDRIZZETTI,** Directeur juridique et conformité, FBF
- **Stéphane PUEL,** Avocat associé, Gide Loyrette Nouel, membre du HCJP
- **Didier REBUT,** Docteur en droit, agrégé des facultés de Droit, Professeur de Droit à l'Université Paris 2 Panthéon-Assas
- **Guillaume RICHARD,** Responsable adjoint du service Banque de Détail, Direction des Affaires Juridiques, Crédit Agricole SA
- **Clément ROBERT,** Adjoint au bureau Bancfin 4, bureau des services bancaires et des moyens de paiement, Direction Générale du Trésor
- **Julien ROSIER,** Adjoint au chef du bureau du droit de l'économie des entreprises, Direction des Affaires Civiles et du Sceau, Ministère de la Justice
- **Thierry SAMIN,** Responsable de la règlementation, Société Générale
- **Laurence THEBAULT,** Responsable juridique, BNP Paribas
- **Nathalie VERGNE,** Adjointe au Chef du Service Droit Bancaire et Missions d'Intérêt Général, Direction des Services Juridiques, Banque de France
- **Hélène WIART,** Responsable du service Banque de Détail, Direction des Affaires Juridiques, Crédit Agricole SA

ANNEXE 2

Étude synthétique sur l'encadrement du secret bancaire au sein de plusieurs pays de l'Union européenne, en Suisse et aux États-Unis

ANNEXE 2

Étude synthétique sur l'encadrement du secrait bancaire au sein de plusieurs pays de l'Union européenne, en Suisse et aux États-Unis

Juridiction	Obligation légale	Fondement juridique	Sanction en cas de violation du secret bancaire
Allemagne	×	• Le secret bancaire ne fait pas l'objet de dispositions légales particulières, mais est établi par la coutume. • Le code pénal allemand prévoit toutefois un certain nombre de dispositions sanctionnant le secret professionnel applicable à certaines professions ou agents de la fonction publique (v. articles 203 et 204).	• Responsabilité contractuelle en cas de violation. • Responsabilité disciplinaire éventuelle si la violation constitue également un manquement aux règles d'organisation de la banque (dans la plupart des cas, uniquement s'il s'agit d'un manquement à une instruction spécifique d'une autorité). • Toutefois, la violation du secret bancaire peut être sanctionnée pénalement si cette violation est commise par un salarié d'une banque relevant du droit public.
Belgique	×	• Il n'existe pas d'obligation légale encadrant spécifiquement le secret bancaire. • Toutefois, un devoir de discrétion a été imposé par la coutume et les usages aux banques et à certaines autres entités régulées dans le cadre de leur relation avec leurs clients. • En outre, il est imposé aux parties à une relation contractuelle d'agir avec bonne foi en toutes circonstances ; une partie de la doctrine en déduit que ce devoir de bonne foi impose aux parties de respecter la confidentialité des informations transmises dans le cadre des négociations précontractuelles.	• Pas de sanction spécifique. • Toutefois, certaines décisions de juridictions belges ont octroyé des dommages moraux en cas de violation du devoir de discrétion.
Espagne	√	Article 83 de la Loi 10/2014 du 26 juin 2014.	• Aux termes de l'article 83 de la Loi 10/2014, le manquement au secret bancaire est qualifié d'infraction grave. Les sanctions applicables aux infractions graves sont prévues à l'article 98 de ladite loi. Ces sanctions sont de nature civile, et peuvent être doublées de sanctions pénales (article 117 de la Loi 10/2014). • Une amende égale à : (i) deux ou trois fois le montant des avantages

Juridiction	Obligation légale	Fondement juridique	Sanction en cas de violation du secret bancaire
			obtenus de la violation, dans le cas où ces avantages peuvent être quantifiés ; ou (ii) entre 3% et 5% du chiffre d'affaires annuel net de la société au cours de l'année précédente, y compris les revenus bruts provenant des intérêts à percevoir et des revenus assimilés, les revenus des actions et autres titres à revenu fixe ou variable et les commissions et honoraires à percevoir ; ou encore (iii) entre 2 000 000 et 5 000 000 euros, si le pourcentage précité est inférieur à ces montants. • Additionnellement à l'amende, les sanctions suivantes peuvent être prononcées : (a) une injonction de cesser le comportement fautif et de s'abstenir de le réitérer ; (b) un avertissement public publié dans le Journal Officiel comprenant l'identité de l'auteur de l'infraction, la nature de l'infraction et les sanctions imposées ; ou (c) un avertissement privé. • Enfin, en plus des sanctions imposées à l'entité en elle-même, l'article 101 de la Loi 10/2014 liste des sanctions à l'encontre de ses dirigeants ou responsables répondant de l'infraction et des personnes ou entités détenant une part significative de l'entité en infraction, ainsi que leurs dirigeants et responsables. La nature de la sanction dépendra de l'infraction, et pourra être, entre autres, un avertissement public, une amende (d'un montant maximum de 2 500 000 euros), une interdiction de gérer ou la révocation ou suspension de ses fonctions pendant une durée limitée. • La Banque d'Espagne a la possibilité de déterminer le montant de l'amende selon un certain nombre de critères définis à l'article 103.

Juridiction	Obligation légale	Fondement juridique	Sanction en cas de violation du secret bancaire
Italie	×	• Il n'existe pas d'obligation légale encadrant spécifiquement le secret bancaire. • Toutefois, il est généralement entendu que les banques ont un devoir implicite de secret bancaire. Le devoir de confidentialité en matière bancaire a été déduit par la doctrine : (i) des principes de bonne foi et d'équité établis par le Code civil italien ; (ii) des recommandations publiées par l'Autorité de protection des données italienne (*Garante per la protezione dei dati personali*) (notamment, les directives pour le traitement des données des clients dans le secteur financier en date du 25 octobre 2007 et la résolution no. 192 du 12 mai 2011 sur le partage des données dans le domaine bancaire) ; et (iii) de la décision no. 51 du 18 février 1992 par la Cour constitutionnelle italienne (*Corte Costituzionale*).	Pas de sanction spécifique.
Luxembourg	√	Article 41 de la loi du 5 avril 1993 sur secteur financier (combiné à l'article 458 du Code pénal luxembourgeois)	Sanction pénale : emprisonnement de huit jours à six mois et amende de 500 à 5 000 euros.
Pays-Bas	×	• Il n'existe pas d'obligation légale encadrant spécifiquement le secret bancaire. • Toutefois, dans le cadre de la relation contractuelle existant entre l'établissement de crédit et ses clients, il existe un devoir de confidentialité implicite au profit des clients, qui interdit à l'établissement de crédit de partager les informations confidentielles du client.	• Pas de sanction spécifique. • Sur le fondement de la responsabilité contractuel, des dommages et intérêts pourraient être accordés.
Pologne	√	Article 104 de la loi bancaire du 29 août 1997 (*ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe*).	Sanction pénale : amende d'un montant maximum de 1 000 000 PLN et emprisonnement pouvant aller jusqu'à trois ans.
Royaume-Uni	×	• Il n'existe pas d'obligation légale encadrant spécifiquement le secret bancaire.	• La FCA peut imposer des amendes illimitées ou infliger un blâme public à la banque ou ses dirigeants.

Juridiction	Obligation légale	Fondement juridique	Sanction en cas de violation du secret bancaire
		• Le secret bancaire est généralement contractuel, issu des termes implicites ou exprès du contrat. • Au surplus, les banques anglaises sont assujetties à des obligations générales découlant des principes édictés par la FCA (*Financial Conduct Authority*), dont l'obligation de traiter les clients équitablement. Une atteinte aux termes contractuels exprès ou implicites ou aux attentes légitimes du client en matière de confidentialité pourra également caractériser une violation des principes de la FCA.	• En outre, il peut exister d'autres conséquences réglementaires, y compris des restrictions aux, une suspension ou un retrait des autorisations de la banque, une suspension ou une révocation d'autorisations individuelles et des injonctions judiciaires ou des injonctions judiciaires d'indemniser les pertes encourues ou de restituer les profits. • Les banques doivent mettre en place une procédure de traitement des réclamations des clients de manière juste et efficace. Par ailleurs, les particuliers et certaines autres catégories de clients (comme les micro-entreprises, certaines petites organisations caritatives et les trusts) peuvent saisir le médiateur de la conduite d'une banque lequel peut octroyer une compensation financière et ordonner des mesures correctives. Le médiateur statue sur les réclamations en se référant à ce qui lui semble juste et raisonnable selon les circonstances. • Enfin, les banques sont assujetties à des obligations en vertu des règles de confidentialité et de protection des données.
Etats-Unis	✕	• Il n'existe pas d'obligation légale encadrant spécifiquement le secret bancaire. • La jurisprudence rendue par les juridictions de l'Etat de New York indique qu'il pourrait exister un devoir de confidentialité de la banque à l'égard de ses clients en qualité de déposants, mais qu'un tel devoir n'existe pas à l'égard des clients emprunteurs. • En outre, il existe plusieurs mesures de protection des données financières au regard du droit fédéral américain pour les personnes ayant obtenu des produits ou services financiers à des fins personnelles, familiales ou domestiques	Pas de sanction spécifique.

Juridiction	Obligation légale	Fondement juridique	Sanction en cas de violation du secret bancaire
		("consommateurs"). Au titre de ces dispositions, les institutions financières américaines ont généralement l'interdiction de divulguer les informations personnelles privées d'un consommateur à des tiers non-affiliés sans donner la possibilité au consommateur de s'opposer à la divulgation. Néanmoins, ce droit ne protège pas la divulgation des informations privées des consommateurs personnes morales. En tout état de cause, ces dispositions ne sont pas considérées comme des règles de secret bancaire. • Il existe également une loi fédérale nommée "Loi pour le droit à la confidentialité des données financières" (*Right to Financial Privacy Act* ("RFPA")), dont l'objectif est de mettre en place des procédures que les autorités américaines doivent suivre pour obtenir de la part d'une institution financière des informations sur la situation bancaire d'un consommateur, et non d'imposer des interdictions de divulgation de données financières de consommateurs aux autorités gouvernementales ou à des tiers.	
Suisse	√	Article 47 de la loi fédérale sur les banques et les caisses d'épargne du 8 novembre 1934.	• Sanction pénale (emprisonnement pouvant aller jusqu'à trois ans et amende). • En outre, l'obtention d'un avantage pécuniaire en raison de la violation du secret bancaire est punie d'un emprisonnement pouvant aller jusqu'à cinq ans ou d'une amende. Si l'auteur agit par négligence, il est puni d'une amende de 250.000 CHF au plus.

ANNEXE 3

Secret bancaire et loi étrangère à portée extraterritoriale : l'exemple du Cloud Act

ANNEXE 3

Étude synthétique sur l'encadrement du secrait bancaire au sein de plusieurs pays de l'union Européenne, en Suisse et aux États-Unis

I- La genèse et les principes du *Cloud Act*

Le *Clarifying Lawful Overseas Use of Data Act* est une loi américaine du 23 mars 2018 amendant la loi SCA (*Stored Communications Act*) de 1986, ce dernier fixant un principe de confidentialité et de protection des données de communication traitées ou stockées par des fournisseurs de services de communication. Le *Cloud Act* doit simplifier et modifier la procédure d'accès aux informations qui nécessitaient un recours aux MLAT (*Mutual Legal Assistant Treaty*).

Le *Cloud Act* est une séquelle d'une affaire dans laquelle Microsoft avait refusé aux autorités US, s'agissant d'une affaire de stupéfiants, l'accès à des données stockées dans un « *data center* » irlandais. Microsoft avait fait valoir que le contenu des courriels, n'appartenant qu'à ses clients, n'était donc pas sous son contrôle et que le gouvernement américain avait pour obligation d'utiliser un mandat de perquisition (warrant), plutôt qu'une citation à comparaître, pour demander la communication du contenu des emails stockés en Irlande.

Le 14 juillet 2017, la Cour d'Appel de New York a donné raison à Microsoft, concluant que le gouvernement américain ne pouvait unilatéralement contraindre Microsoft à lui donner accès à des données stockées exclusivement en dehors des États-Unis et devait dès lors faire appel aux traités d'assistance judiciaire mutuelle et qu'un mandat de perquisition n'était pas suffisant.

Sans attendre la décision de la Cour Suprême[153] saisie par le *Departement Of Justice*, le gouvernement a adopté un texte prévoyant en présence de « *serious crime* »[154], un droit de communication au bénéfice des autorités américaines de diverses données, sans considération du lieu où ces données sont stockées. Bien entendu, les sociétés « incorporées » aux Etats-Unis, et celles que ces dernières contrôlent, sont les plus directement concernées.

Le *Cloud Act* permet aux autorités américaines, dans le cadre d'enquêtes judiciaires criminelles, d'obtenir des données stockées en dehors des États Unis, le § 2713 de ce texte visant « *[…] tout*

[153] *Laquelle s'est élevée à plusieurs reprises contre l'extraterritorialité des lois US : en 2010, dans l'affaire Morrison v. National Australia Bank (24 juin 2010) la Cour suprême affirme, de manière générale, un principe de droit américain de présomption contre l'extraterritorialité (presumption against extraterritoriality), d'où il ressort que sauf volonté explicite du Congrès, une loi n'a pas une portée extraterritoriale. Idem, Kiobel v. Royal Dutch Petroleum, 17 avril 2013 ou bien encore, OBB Personenverkehr AG v. Sachs, 1er décembre 2015. Les amicus brief du Parlement Européen et du Conseil des barreaux européens sont disponibles aux adresses suivantes : http://bit.ly/2EclkMD (PE) et http://bit.ly/2DFlfE3 (CCBE).*

Cloud Act : Sec.2. Congressional findings - Cf.infra § 6.

enregistrement ou autre information concernant un client ou un abonné en sa possession, la garde ou le contrôle, que cette communication, cet enregistrement ou d'autres informations se trouvent à l'intérieur ou à l'extérieur des États-Unis »[155]. Ce faisant, ce texte simplifie et modifie la procédure d'accès aux informations, qui nécessitait un recours aux MLAT *(Mutual Legal Assistant Treaty)*[156], *dans une démarche qui, pour les autorités américaines, ne relève pas de l'effet extraterritorial des textes.*

(i) *Les entreprises concernées*

La rédaction du § 2713 du SCA est compréhensive en ce qu'elle vise les « *providers of electronic communications services or remote computing services* »[157] et vise les données qui sont en dehors des USA et « *in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States* ». Aucune limitation ne permet de restreindre son emprise aux seules entreprises américaines traitant ou hébergeant des données hors du territoire des États Unis.

(ii) *Les personnes concernées*

En principe, les *US persons* devraient être les seules concernées. En pratique les choses sont différentes. Dans un premier temps, toutes les personnes, et pas uniquement les « *US persons* » telles que définies par le *Cloud Act*[158], peuvent être visées. La prise en considération de la nationalité de la personne visée par la demande de communication n'intervient que dans un second temps, à titre d'exception pourrait-on dire, lors de la contestation que peut soulever le prestataire[159]. Ainsi, le *Cloud Act* peut concerner les données de personnes physiques, peu importe qu'elles soient ou non de nationalité américaine ou qu'elles résident ou pas sur le territoire de États Unis.

---

[155] *§ 2713 : "Required preservation and disclosure of communications and records". Le texte precise " […] à propos de la communication des données : "regardless of whether such communication, record, or other information is located within or outside of the United States".*

[156] *Accords d'assistance juridique mutuelle.*

[157] *Définis par l'Electronic Communications Privacy Act de 1986 ; cf. l'United States Code, titre 18, § 2510(12) et 2711(2). Concerne les opérateurs de communications électroniques dont l'offre d'accès wifi publics, mais aussi les opérateurs de cloud computing.*

[158] *§ 2523 : "Executive agreements on access to data by foreign governments - (a) DEFINITIONS.—In this section: "US person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an un incorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States".*

[159] *§ 2713 (h) (2) (A) du Cloud Act : "A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes:*
(i) that the customer or subscriber is not a United States person and does not reside in the United States; and
(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government".

(iii) *Les crimes et délits concernés par le Cloud Act*

Le *Cloud Act* vise les efforts du gouvernement pour protéger la « *public safety* » et combattre les « *serious crime, including terrorism* »[160]. On notera par ailleurs que, dans le reste du texte, la notion de « *serious crime* » n'apparaît plus que s'agissant des demandes de communication tournées vers les États-Unis[161]. Il s'en suit que les autorités US pourraient adresser des demandes de communication au sujet d'infractions très variées, relevant de la notion floue de « sécurité publique ».

En ce qui concerne les *serious crimes*, si le code fédéral (18 USC 2703[162]) précise que les requêtes des autorités gouvernementales ne peuvent se faire que dans le cadre de la procédure criminelle prévue par ce code, le *Cloud Act* vise spécifiquement les « *serious crime, including terrorism* », ainsi que la notion de « *threat of death or serious bodily harm to any person* »[163]. La question qui se pose est celle du périmètre de ces *serious crimes*. À titre d'exemple, l'article 37 du CFR (*United States Code of Federal Regulations*) donne la définition suivante :

- "Any criminal offense classified as a felony[164] under the laws of the United States, any state or any foreign country where the crime occurred; or

- Any crime a necessary element of which, as determined by the statutory or common law definition of such crime in the jurisdiction where the crime occurred, includes interference with the administration of justice, false swearing, misrepresentation, fraud, willful failure to file income tax returns, deceit, bribery, extortion, misappropriation, theft, or an attempt or a conspiracy or solicitation of another to commit a serious crime."

Ce même article 37 du CFR donne la définition suivante des « *serious crime* » : "*Any criminal offense classified as a felony[165] under the laws of the United States, any state or any foreign country where the crime occurred*".

Cette énumération ne permet pas de connaître avec précision les crimes et délits pouvant donner lieu à recours au *Cloud Act*, on peut donc en déduire une réelle exposition au fait que des données couvertes par le secret bancaire puissent être concernées.

---

[160] *§ 2523. Executive agreements on access to data by foreign governments - DEFINITIONS.—In this section, spec. D.*

[161] *Cf. section 5 -3- D et les commentaires de P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières. - Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », Cahiers de droit de l'entreprise, Juill. 2018 du 1er Juillet 2018.*

[162] *L'United States Code constitue l'équivalent de notre code pénal et de notre code de procédure pénale réunis. Il comprend un chapitre 121 connu sous le nom de Stored Communications Act (le « SCA »).*

[163] *Ibid. G.*

[164] *De manière générale, infraction passible d'une peine d'emprisonnement supérieure à un an.*

[165] *Délit passible d'un emprisonnement supérieur à un an.*

(iv) *Application extraterritoriale du Cloud Act*

Le *Cloud Act* permet aux autorités américaines, dans le cadre d'enquêtes judiciaires criminelles, d'obtenir des données stockées en dehors des États Unis, le § 2713 de ce texte visant « *[…] tout enregistrement ou autre information concernant un client ou un abonné en sa possession, la garde ou le contrôle, que cette communication, cet enregistrement ou d'autres informations se trouvent à l'intérieur ou à l'extérieur des États-Unis* »[166]. Ce faisant, ce texte simplifie et modifie la procédure d'accès aux informations, qui nécessitait un recours aux MLAT (*Mutual Legal Assistant Treaty*)[167], dans une démarche qui, pour les autorités américaines, ne relève pas de l'effet extraterritorial des textes.

Pour le DOJ, le *Cloud Act* est un instrument d'uniformisation des règles internationales de production des preuves, ce dernier évoquant à diverses reprises, dans un white paper intitulé « *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act* »[168], la suppression des obstacles issus des législations nationales.

Ce document énonce ainsi : « *Le Cloud act représente donc un* ***nouveau paradigme*** *: une approche efficace et protectrice de la vie privée à l'égard de la sécurité publique en améliorant l'accès efficace aux données électroniques dans le cadre des autorisations légales existantes* » – (white paper – introduction p.2). Par la suite, cette volonté d'uniformisation du droit est clairement rappelée :

• « *Supprimer les restrictions prévues par les lois de chaque pays* » (WP p. 3) ;

• « *Les États-Unis et tout partenaire d'un accord Cloud Act conviendraient de supprimer les restrictions légales imposées aux fournisseurs pour qu'ils se conforment aux ordonnances émises en vertu de l'accord dans les circonstances que les deux pays jugent appropriées* » - (WP - FAQ § 4[169]).

La doctrine du gouvernement américain peut se résumer ainsi : dès lors que des données sont accessibles depuis les États-Unis, fussent-elles stockées hors de ces mêmes États-Unis, elles sont supposées se trouver « à portée de clic » et, par une fiction « juridico-technique », être sur le sol américain. Au cours de la procédure opposant Microsoft à l'État américain, ce dernier a souligné : « *Microsoft's U.S. based employees could make that disclosure without leaving their desks* »[170]. La question n'est donc pas où se trouvent les données, mais d'où sont-elles accessibles. Cette approche

[166] *§ 2713 : "Required preservation and disclosure of communications and records". Le texte precise […] à propos de la communication des données : "regardless of whether such communication, record, or other information is located within or outside of the United States ".*

[167] *Accords d'assistance juridique mutuelle.*

[168] *www.justice.gov/CLOUDAct*

[169] *https://www.justice.gov/dag/page/file/1153466/download*

[170] *https://www.wsj.com/articles/supreme-court-to-hear-microsoft-case-on-emails-customer-data-stored-overseas-1519641001*

peu de cas du fait que les données transmises ont été préalablement physiquement stockées, en un lieu géographique précis.

II- Les sources de conflits avec le RGPD

Nous en retiendrons 4 qui serviront d'illustration au fait que la question de la compatibilité avec le secret bancaire des demandes sous couvert du *Cloud Act* est concurrente de l'examen de la compatibilité avec les dispositions du RGPD. Ce constat permet de distinguer les incompatibilités relatives à un « ordre public de protection particulier » (le secret bancaire), de celles liées à un ordre public de protection générale. Cette dernière incompatibilité constituant, à elle seule, un obstacle dirimant à toute communication d'information.

(i) Première source de conflit : licéité du traitement - Absence d'information et donc de base légale au traitement (consentement préalable) ;

(ii) deuxième source de conflit : régime des transferts de données hors UE en vertu de l'article 48 du RGPD ;

(iii) troisième source de conflit : exception à l'article 48 du RGPD – Application de l'article 49 ;

(iv) quatrième source de conflit : application extraterritoriale du RGPD.

S'agissant du secret bancaire, la question qui se pose de manière continue est celle de la « légitimité juridique » des demandes présentées sous l'égide du *Cloud Act*. En effet, outre la question du périmètre d'application de ce texte, se pose aussi la question du caractère occulte des demandes, en dépit des exceptions évoquées par le DOJ[171]. Cette dimension occulte ne permet bien évidemment pas d'opposer une quelconque exception, qu'elle soit liée au secret ou à la loi de blocage.

Par ailleurs, ces demandes sont incompatibles avec diverses dispositions d'ordre public (outre le RGPD, on mentionnera la loi dite de blocage[172]).

Nous partirons du postulat suivant :

- la levée du secret bancaire devient une question « contingente », dès lors que les demandes présentées par les autorités US sont contraires à des dispositions de protection de l'ordre public au sens le plus large du terme ;
- la contrariété à des dispositions d'ordre public des demandes de communication de données présentées sous l'empire du *Cloud Act* conduit à estimer que ces dernières ne peuvent être considérées comme dérogatoires au secret bancaire.

[171] *Cf. Infra : Le recueil du consentement – article 6 §1 pt a.*

[172] *Loi n° 68-678 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

La démarche consiste donc à rechercher un fondement légal légitime à la demande des autorités US, puis à évaluer dans quelle mesure le secret bancaire est susceptible de s'appliquer.

(i) Première source de conflit : licéité du traitement - Absence d'information et donc de base légale (ex : consentement préalable)

L'article 6 du RGPD prévoit, outre le consentement[173], divers motifs permettant de retenir la licéité d'un traitement :

- Art. 6-1 – b) traitement nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

- c) traitement nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis ;

- d) traitement nécessaire à la **sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne physique ;

- e) traitement nécessaire à **l'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

- f) traitement est nécessaire aux fins **des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Nous exclurons le point b relatif à l'exécution d'un contrat.

- Le recueil du consentement – article 6 §1 pt a

Le *Cloud Act* permet d'accéder aux données personnelles des personnes physiques sans leur consentement, puisqu'aucune information de ces dernières n'est prévue. Le critère de licéité des traitements reposant sur le consentement (art. 6-1 a) préalable de la personne physique n'est donc pas applicable.

---

[173] Art. 6-1 – b) traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci – c) traitement nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis – d) traitement nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique – e) traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

On notera toutefois que, s'agissant de l'information des personnes, non pas celles directement objets des demandes de communication au travers du *Cloud Act*, mais celles détentrices de ces données, le département de la Justice US apporte une précision dans son « *white paper* » d'avril 2019 consacré à « L'objet et l'impact du *Cloud Act* »[174].

Ce document précise (White paper - Q&A 28): "*Providers may notify account holders of searches pursuant to a U.S. court order under the Stored Communications Act unless an independent judge has issued a protective order*"[175].

Une ordonnance de protection intervient lorsque le juge indépendant détermine qu'il y a lieu de croire que la notification de l'existence de l'ordonnance pourrait compromettre la poursuite de l'enquête ou la tenue d'un procès (intimidation de témoins, vol ou falsification de documents, etc.).

En tout état de cause, même si une telle information avait lieu de manière générale et anticipée, on ne pourrait en déduire *ipso faco* un consentement au sens de l'article 4 du RGPD, c'est-à-dire : « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Le consentement doit donc être spécifiquement donné pour le transfert concerné. Ainsi, le consentement préalable de la personne concernée par un futur transfert, si la survenance et les circonstances particulières de ce transfert ne sont pas connues au moment où le consentement est demandé, ne permet pas de mesurer l'incidence sur la personne concernée de l'autorisation donnée. Ladite autorisation ne peut être retenue[176].

S'agissant des responsables de traitement, leur information n'est pas non plus envisagée par le *Cloud Act*. Toutefois, le DoJ permet, sous condition, une telle information : "*In general, as explained below, prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation*"[177]. - (Directive interne p. 1, 1er §[178]).

---

[174] *www.justice.gov/CLOUDAct*

[175] *« Les fournisseurs peuvent aviser les titulaires de comptes des recherches effectuées en vertu d'une ordonnance d'un tribunal américain en vertu de la Stored Communications Act, à moins qu'un juge indépendant n'ait rendu une ordonnance de protection ».*

[176] *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679Adopted on 25 May 2018 spéc. § 2.1.2. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf*

[177] *« En général, comme expliqué ci-dessous, les procureurs devraient demander des données directement à l'entreprise, plutôt qu'à son fournisseur de stockage en nuage, si cela ne compromet pas l'enquête ».*

[178] *https://www.justice.gov/criminal-ccips/file/1017511/download*

Le caractère occulte de la demande présentée dans le périmètre du *Cloud Act* exclue que la personne concernée puisse manifester un quelconque consentement à la levée du secret bancaire. Resterait à envisager une levée à raison d'une des exceptions légales en la matière. La seule exception envisageable est celle liée à une procédure pénale (art. L.511-33 al. 2 et L.522-19 al. 2 du Code monétaire et financier), cette dernière n'est pas applicable ici (cf. *infra*).

- La nécessité du traitement afin de respecter une obligation légale à laquelle le responsable du traitement est soumis – article 6 § 1, pt c

En vertu de l'article 6, paragraphe 3, du RGPD[179] ce fondement devrait avoir pour base légale le droit de l'Union ou des États membres. Conformément à l'article 48 du même règlement, la demande présentée par une autorité judiciaire ne peut produire ses effets que si elle est fondée sur un accord international, tel un traité d'entraide judiciaire, conférant à cette demande des effets contraignants.

Un motif de licéité sous le visa de l'article 6 § 1, pt c ne pourra être issu que d'un futur accord bilatéral entre l'UE et les États-Unis, que la Commission européenne s'apprête à négocier[180]. Dans cette attente, la levée du secret bancaire ne peut se justifier dans un tel contexte.

À cet égard, l'examen de la question de l'opposabilité du secret bancaire, secret de protection, devrait nous semble-t-il tenir compte des autres textes d'ordre public poursuivant également un tel objectif mais sur un périmètre plus étendu que la relation bancaire. Dès lors, le secret bancaire ne devrait être levé en présence de demandes, fussent-elles de nature judiciaire, présentant un défaut de conformité avec des dispositions d'ordre public.

L'exception au secret issue du Code monétaire et financier au titre d'une demande de « *l'autorité judiciaire agissant dans le cadre d'une procédure pénale* » ne peut valoir qu'autant que cette autorité agisse dans le respect de l'ordre public interne.

---

[179] « *Le fondement du traitement visé au paragraphe 1, points c) […] est défini par: a) le droit de l'Union; ou b) le droit de l'État membre auquel le responsable du traitement est soumis. Les finalités du traitement sont définies dans cette base juridique […]* ».

[180] *Le 6 juin 2019, le Conseil a donné mandat à la Commission européenne pour négocier au nom de l'Union européenne un accord avec les Etats-Unis afin de faciliter l'accès aux preuves électroniques aux fins de la cooperation judiciaire en matière pénale. Ceci fait suite à la publication de la recommandation https://www.consilium.europa.eu/fr/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/*

- La protection des intérêts vitaux d'une personne autre que la personne concernée – article 6 § 1 pt d

Ce motif pourrait viser une demande d'une autorité hors UE, présentée dans un conteste de danger imminent et avéré, pour la vie ou l'intégrité physique d'autres personnes, dans un pays tiers. Toutefois, le considérant 46 du RGPD précise que le transfert de données à caractère personnel « *fondé sur l'intérêt vital d'une autre personne physique ne devrait en principe avoir lieu que lorsque le traitement ne peut être manifestement fondé sur une autre base juridique* ».

Dans le cas des demandes présentées sous le visa du *Cloud Act*, il existe en principe une autre base juridique permettant de tels transferts, en relation avec des textes prévoyant la poursuite et la répression d'une infraction.
En présence de demandes, dont la conformité à des textes d'ordre public est contestable, et ne bénéficiant ainsi d'aucun régime dérogatoire au secret bancaire, ce dernier a pleinement vocation à s'appliquer.

- Mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement - article 6 § 1 pt e

Encore une fois, les intérêts ou l'exercice de l'autorité publique, conformément à l'article 6, paragraphe 3, du RGPD, ne visent que ceux ayant pour base le droit de l'Union ou des États membres. Au cas d'espèce, les demandes présentées sous l'égide du *Cloud Act* ne peuvent être considérées comme satisfaisant cette condition.

Par ailleurs, la mise en œuvre de la réglementation LCBFT doit être vue comme la satisfaction d'une obligation légale[181] et non comme l'exécution d'une mission d'intérêt public[182], l'une et l'autre de ces deux notions constituant des fondements juridiques distincts au regard du RGPD.

Toutefois, en matière de portabilité, le G29[183] mentionne la LCB-FT et énonce : « *les établissements financiers n'ont pas l'obligation de donner suite à une demande de portabilité des données concernant les données à caractère personnel traitées dans le cadre de* ***leurs obligations*** *en matière de prévention et de détection du blanchiment d'argent et d'autres formes de criminalité financière* ».

[181] *Article 6-c du RGPD qui vise une « obligation légale à laquelle le responsable du traitement est soumis ».*

[182] *Article 6-e du RGPD.*

[183] *Lignes directrices relatives au droit à la portabilité des données - Adoptées le 13 décembre 2016 - Version révisée et adoptée le 5 avril 2017 - WP 242 rev.01, spéc. p. 10.*

Or, l'article 20-3 du RGPD vise au titre des exceptions à la portabilité le « *[…] traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement* ». Il existe donc une confusion entre « obligations légales » et « mission d'intérêt public ».

Les remarques ci-dessus, relatives à la compatibilité des demandes sous l'empire du *Cloud Act* avec l'ordre public, valent à l'identique. Il ne semble pas envisageable de lever le secret bancaire au bénéfice de demandes présentant par ailleurs d'importantes irrégularités réglementaires au regard notamment du RGPD.

- Intérêt légitime poursuivi par le responsable du traitement ou par un tiers à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel […] - article 6 § 1 pt f

La notion d'intérêt légitime du responsable du traitement (ou de tiers) doit être mis en balance avec les intérêts ou les droits et libertés fondamentaux de la personne concernée[184]. Le résultat du test de mise en balance détermine si l'article 6, paragraphe 1, point f)[185] peut être invoqué comme base juridique du traitement.

La notion de « *libertés et droits fondamentaux de la personne concernée* » vise directement la compatibilité avec la protection accordée par l'article 47 de la Charte des droits fondamentaux de l'Union européenne prévoyant, notamment, un droit à un recours effectif qui semble impossible à exercer en l'absence de transparence de la procédure. Une fois encore, le secret bancaire a pleinement vocation à s'appliquer.

o *Prévention d'infractions pénales (« serious crimes » au sens du Cloud Act) versus…*

Un responsable du traitement peut avoir un intérêt légitime à déférer à une demande de divulgation de données à caractère personnel sous le visa du *Cloud Act*. Cet intérêt repose tant sur les obligations légales de concours à la lutte contre diverses formes de criminalité (LCBFT, corruption ; etc.), que sur les risques de sanctions en cas de refus de communication.

[184] *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE – 9 avril 2014.*

[185] *Avis 06/2014, spéc. p 26.*

Le RGPD considère que « *Le traitement de données à caractère personnel strictement nécessaire à des fins de prévention de la fraude constitue également un intérêt légitime du responsable du traitement concerné* » et que « *[…] révéler l'existence d'éventuelles infractions pénales ou de menaces pour la sécurité publique et de transmettre à une autorité compétente les données à caractère personnel concernées dans des cas individuels ou dans plusieurs cas relatifs à une même infraction pénale ou à des mêmes menaces pour la sécurité publique devrait être considéré comme relevant de l'intérêt légitime du responsable du traitement…[…]* »[187].

Toutefois, les autorités US aptes à présenter des demandes de communication au titre du *Cloud Act* ne sont pas des autorités publiques ou compétentes établies en vertu du droit communautaire (cf. article 6, paragraphe 3 du RGPD). Par ailleurs, le caractère contraignant des demandes présentées sous le visa du *Cloud Act* empêche les responsables de traitement de respecter leurs obligations issues des droits reconnus par le RGPD, dont notamment le droit d'accès et opposition.

o … *Intérêts ou droits et libertés fondamentaux de la personne concernée*

L'évaluation de l'impact sur les intérêts de la personne concernée doit tenir compte de toutes les conséquences du traitement des données personnelles, notamment au regard des attentes raisonnables de ladite personne[188].

S'agissant du *Cloud Act*, les demandes d'accès des autorités US auront lieu, en l'absence d'accord international, sans que puisse être évaluée la compatibilité avec la protection accordée par l'article 47 de la Charte des droits fondamentaux de l'Union européenne prévoyant, notamment, un droit à un recours effectif qui semble impossible à exercer en l'absence de transparence de la procédure. On notera que le 3 octobre 2019, les États-Unis et le Royaume-Uni ont adopté un projet d'accord bilatéral sur le transfert de données dans le cadre du *Cloud Act*[189]. Si la signature d'un tel accord (Executive Agreement) avec un « *qualifying foreign government* » (QFG) n'est pas une condition de mise en application du *Cloud Act*, il présente l'avantage d'être l'une des deux conditions cumulatives

[186] *Considérant 47 in fine.*

[187] *Considérant 50 in fine.*

[188] *Considérant 47 : « En tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée ».*

[189] *https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate. Au sujet de cet accord, E. Jouffin, « Cloud Act - Accord bilatéral USA-UK : les anglais ont tiré les premiers », Banque et Droit n° 189, p. 4.*

nécessaires pour qu'un fournisseur de services puisse s'opposer à une demande de communication de données[190].

Ici encore, des considérations d'ordre public devraient conduire à exclure toute communication d'information dans le contexte du *Cloud Act*, refus motivé par des arguments de portée plus large que la question du secret bancaire.

(ii) Deuxième source de conflit : régime des transferts de données hors UE en vertu de l'article 48 du RGPD

Pour le gouvernement américain, la prise de connaissance des données n'intervenant qu'au moment où s'effectue la prise de connaissance des mails expédiés aux USA, cette divulgation se déroule sur le territoire américain et, par voie de conséquence, seule la loi américaine est applicable, indépendamment du lieu d'extraction des données. Cette doctrine n'est pas compatible avec les dispositions de l'article 48 du RGPD.

Le RGPD interdit le transfert direct de données personnelles hors UE, sauf existence d'un accord international. L'article 48 du RGPD (« *Transferts ou divulgations non autorisés par le droit de l'Union* ») prévoit que « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ».

Pour la Commission européenne, « *l'article 48 précise clairement qu'une décision d'un tribunal étranger ne rend pas, en tant que telle, un transfert licite dans le cadre du RGPD* »[191].

S'agissant du *Cloud Act*, en l'absence d'un « *executive agreement* », c'est-à-dire d'un accord bilatéral signé avec un « *qualifying foreign government* » (QFG)[192] le transfert de données ne satisfait pas aux exigences du RGPD.

---

[190] *§ 2713. "Required preservation and disclosure of communications and records": "A provider of electronic communication service to the public or remote computing service, […] may file a motion to modify or quash the legal process where the provider reasonably believes: "(i) that the customer or subscriber is not a United States person and does not reside in the United States; and "(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.*

[191] *Amicus Curiae dans USA v. Microsoft corporation p. 14. https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf*

[192] *Pour être QFG, un état devra satisfaire à un ensemble d'exigences très détaillées visées au § 2523 du Cloud Act ((b) Executive agreement requirements), lesquelles sont satisfaites par application du RGPD.*

Dans ses lignes directrices sur l'article 49, le Comité Européen à la Protection des Données[193] précise qu'en l'absence d'accord international, tel qu'un traité d'entraide judiciaire, les entreprises de l'UE devraient généralement refuser les demandes directes et renvoyer l'autorité du pays tiers demandeur à un traité ou accord d'entraide judiciaire existant. Pour le CEPD, l'existence de traités d'entraide multilatéraux doit garantir que les données personnelles divulguées le sont conformément au droit communautaire, et sous le contrôle des tribunaux de l'UE.

L'examen de la compatibilité avec l'article 48 permet d'exclure un quelconque transfert de données sous l'empire du *Cloud Act*, indépendamment de la question de l'opposabilité du secret bancaire. Une fois encore, ce dernier ne saurait être levé au bénéfice de demandes ne respectant pas l'ordre public.

(iii) Troisième source de conflit : exception à l'article 48 du RGPD – Application de l'article 49

- Transferts justifiés par un « motif d'intérêt public »

L'article 49 -1 du RGPD permet un transfert en l'absence de décision d'adéquation, ou de garanties appropriées, y compris de règles d'entreprise contraignantes (BCR), pourvu que puisse être invoquée l'une des exceptions qu'il énonce, dont notamment l'existence d'« *un motif d'intérêt public* » (article 49 d).

Si la lutte contre les « *serious crimes* » est bien d'intérêt public, il ne faut pas lire cette exception de manière extensive.

En ce qui concerne les *serious crimes*, si le code fédéral (18 USC 2703) précise que les requêtes des autorités gouvernementales ne peuvent se faire que dans le cadre de la procédure criminelle prévue par ce code, le *Cloud Act* vise spécifiquement les « *serious crime, including terrorism* »[194], ainsi que la notion de « *threat of death or serious bodily harm to any person* »[195]. Il n'existe pas de définition claire des serious crimes permettant de déterminer précisément la nature des infractions concernées.

Tout d'abord, le considérant 115 du RGPD souligne que l'application extraterritoriale de lois, règlements et autres actes « *peut être contraire au droit international et faire obstacle à la protection*

[193] *Lignes directrices 2/2018 sur les dérogations à l'article 49 du règlement 2016/679, p. 5.*

[194] *"§ 2523. Executive agreements on access to data by foreign governments - DEFINITIONS.—In this section, spec. D.*

[195] *Ibid. G.*

des personnes physiques garantie dans l'Union par le présent règlement. Les transferts ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies ». Sont ici visées des garanties suffisantes relatives à la protection des données personnelles. En présence de demandes sous le visa du *Cloud Act*, les garanties offertes paraissent limitées.

Par ailleurs, ce même considérant vise une divulgation nécessaire « *pour un motif important d'intérêt public reconnu par le droit de l'Union ou le d'un État membre auquel le responsable du traitement est soumis* ». Encore une fois, cette exception, qui est celle de l'article 49 d), ne vaut que s'agissant des intérêts publics d'un des États membres de l'Union ou de l'Union elle-même.

On remarquera enfin que le CEPD[196] souligne que l'existence d'un accord ou d'une convention internationale prévoyant une coopération pour favoriser cet objectif « *peut constituer un indicateur pour évaluer l'existence d'un intérêt public conformément à l'article 49, paragraphe 1, point d)* ». Il ne s'agit donc que d'un point de départ d'une évaluation, et non d'un élément valant, per se, blanc-seing automatique aux fins de transferts de données vers des pays tiers.

Même remarque que ci-dessus.

- Transferts justifiés par la constatation, l'exercice ou à la défense de droits en justice

L'article 49- e) du RGPD, les données à caractère personnel peuvent être transférés vers un pays tiers si elles sont « *nécessaires à l'établissement, à l'exercice ou à la défense de créances en justice* ». Le considérant 111 prévoit la possibilité de transferts dans certains cas où la personne concernée a donné son consentement explicite, « *lorsque le transfert est occasionnel et nécessaire dans le cadre d'un contrat ou d'une action en justice [sans plus de précision sur la nature de telles actions], qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, y compris de procédures devant des organismes de régulation.* » (Considérant 111 du RGPD).

Comme l'expliquent les lignes directrices du Comité Européen de la Protection des Données[197], un lien étroit est nécessaire entre un transfert de données, la procédure spécifique le réclamant et la dérogation. Celle-ci ne peut être utilisée pour justifier le transfert de données à caractère personnel

[196] *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 publiées le 25 mai 2018, issues du Comité européen de la protection des données.*

[197] *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679Adopted on 25 May 2018 spéc. § 2.5, p. 13. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf*

en raison de la simple possibilité qu'une procédure judiciaire ou formelle puisse être engagée à l'avenir. À cet égard, se pose la question de l'application éventuelle de « *lois de blocage* »[198], interdisant ou limitant le transfert de données à caractère personnel à des juridictions étrangères, voire à d'autres organismes officiels étrangers[199].

Cette exception ne peut donc être invoquée de manière générale et par anticipation.

L'exclusion d'un consentement général par anticipation, au titre du RGPD, à ce type de divulgations d'information souligne la fragilité que pourrait représenter une clause par laquelle les clients consentiraient, par avance, à la levée du secret bancaire. En tout état de cause, des considérations de conformité à l'ordre public s'opposeraient à pareille levée du secret.

- Transferts justifiés par l'intérêt légitime « impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée … » (art. 41 § 1 dernier alinéa)

Les conditions d'application cumulative de cet article sont strictes :

- il faut non seulement un intérêt légitime impérieux poursuivis par le responsable du traitement ;
- ce dernier ne prévalant pas sur les intérêts ou les droits et libertés des personnes concernées et ;
- le responsable du traitement doit :
    - o évaluer toutes les circonstances entourant le transfert de données[200] ; et
    - o offrir, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel ;
- le responsable du traitement informe :
    - o l'autorité de contrôle du transfert ;
    - o en vertu des articles 13 et 14 du RGPD les personnes concernées du transfert et des intérêts légitimes impérieux qu'il poursuit.

[198] *À la suite du rapport Gauvain, une réforme de la loi n° 68-678 du 26 juillet 1968, dite « loi de blocage » est en cours..*

[199] *Ibid. p 14.*

[200] *On pense à la mise en place d'une AIPD (analyse d'impact sur la protection des données) visée par l'article 35 § 1, du RGPD. Une AIPD est nécessaire lorsque le traitement est « susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques ».*

En particulier, l'article 49, paragraphe 1, dernier alinéa, impose un certain nombre de conditions cumulatives, parmi lesquelles la mise en place de garanties appropriées par le responsable du traitement lors du transfert des données et l'obligation de notifier à la fois l'autorité de contrôle et la personne concernée du transfert et des intérêts légitimes impératifs poursuivis. Or, le *Cloud Act* paraît difficilement compatible avec de telle garanties, notamment en présence « d'ordonnances de protection » visant à préserver le secret de la demande.

Une fois encore, la question de la levée du secret bancaire ne peut se poser en présence de demandes « originellement viciées » sous l'angle du respect de règles impérieuses d'ordre public.

(iv) Quatrième source de conflit : application extraterritoriale du RGPD

Les fournisseurs américains de services numériques soumis au *Cloud Act* peuvent également être soumis au RGPD. Ce dernier (article 3) s'applique, indépendamment de la question du lieu où s'exerce le traitement et de la nationalité du titulaire des données, à toute personne se trouvant sur le territoire de l'UE. Ainsi, un touriste ou un étudiant américain est protégé par le RGPD lorsqu'il séjourne en France, indépendamment de sa nationalité ou de son lieu de résidence, critères qui sont ceux du *Cloud Act*.

Par ailleurs, sont sous l'emprise du RGPD, outre les responsables de traitements et sous-traitants présents sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union, ceux qui, bien que n'étant pas présent sur le territoire de l'Union, traitent les donnes de personnes s'y trouvant, lorsque les activités sont liées à une offre de biens ou de services (gratuites ou non) ou au suivi du comportement, sur le territoire de l'Union, de ces personnes.

III- Conclusion

En l'absence d'un accord international contenant des garanties solides s'agissant de la protection des données personnelles et, plus largement des droits fondamentaux, la compatibilité du *Cloud Act* avec les principes du RGPD n'est pas établie.

Le secret bancaire, secret de protection, n'a pas vocation à être levé en présence de demandes de communication de données présentant une incompatibilité avérée avec des dispositions d'ordre public, au premier rang desquelles se trouve le RGPD.

Cette incompatibilité a été démontrée dans un avis demandé par la commission LIBE auprès du Comité Européen à la Protection des Données et du Contrôleur européen à la protection des données[201] au sujet des conséquences du *Cloud Act* sur la protection des données personnelles des Européens[202].

Dans leur avis conjoint[203], ces deux autorités soulignent que le *Cloud Act* soulève d'importantes questions de compatibilité avec le RGPD, notamment en ce qui concerne l'application des articles 48 et 49. Par ailleurs, elles réclament que le futur accord bilatéral soit assorti de « *fortes garanties procédurales et de garde-fous solides pour protéger les droits fondamentaux* ».

Toujours en ce qui concerne la compatibilité du *Cloud Act* avec l'ordre public, le rapport Gauvain et, plus récemment, le document sur « *la stratégie nationale du renseignement* » issu de la Coordination Nationale du Renseignement et de la lutte contre le terrorisme »[204] de juillet 2019 soulignent les menaces potentielles de ce texte sur les intérêts de la Nation.

Ainsi, le document sur la stratégie de renseignement souligne :

« *L'édiction, par des États ou des entités non-étatiques, de normes y compris à portée extraterritoriale, peut s'accompagner d'actions d'influence agressives dans les instances de production des normes.*

On assiste par ailleurs à un développement des enquêtes d'autorités judiciaires étrangères à l'encontre des entreprises françaises commerçant à l'international sur la base de lois offensives à portée extraterritoriale. Ces procédures contentieuses ont fréquemment pour effet – recherché ou non – de contraindre les entreprises visées à transférer des actifs essentiels à leur prospérité (informations confidentielles relatives aux dirigeants, clients et fournisseurs, informations financières, brevets et savoir-faire technologiques…), ou à se retirer de certains marchés ».

S'agissant des données chiffrées faisant l'objet d'une demande de communication, le *Cloud Act* est étranger au chiffrement. De ce point de vue, le DOJ est clair, le *Cloud Act* est "encryption-neutral" (white paper FAQ 29)[205]. Les prestataires ne sont donc tenus, ni de déchiffrer les contenus qu'ils

---

[201] *Autorité de contrôle indépendante ayant pour mission de veiller à ce que les institutions et organes de l'UE respectent le droit à la vie privée et à la protection des données lorsqu'ils traitent des données à caractère personnel.*

[202] *Ainsi que le mandat donné à l'UE pour négocier un accord bilatérale avec les États-Unis sur l'accès transfrontalier aux preuves numériques.*

[203] *https://edpb.europa.eu/news/news/2019/twelfth-plenary-session-guidelines-video-surveillance-implications-us-cloud-act_fr*

[204] *https://www.economie.gouv.fr/files/20190703-cnrlt-np-strategie-nationale-renseignement.pdf*

[205] *«It [le Cloud Act] does not create any new authority for law enforcement to compel service providers to decrypt communications. Neither does it prevent service providers from assisting in such decryption, or prevent countries from addressing decryption requirements in their own domestic laws» – Idem pour les accord bilatéraux accords bilatéraux (white paper p. 5).*

détiennent, ni d'ouvrir des portes dérobées permettant un accès aux systèmes d'information. L'exposé des motifs de l'accord bilatéral entre les USA et le UK ne déroge pas à ce principe[206].

Enfin, le principal écueil à l'opposabilité du secret bancaire demeure d'ordre pratique. Le *Cloud Act* ne prévoit en effet pas que les demandes de communication d'information adressées aux prestataires puissent donner lieu à une information des responsables de traitement ou des personnes concernées.

Suggestion :

Le groupe de travail appelle l'attention des pouvoirs publics sur la nécessité, dans le contexte des travaux en cours en France, en Europe et à l'international, sur la nécessité d'une défense de la transparence dans le déroulement des procédures de communication de preuves par voie électronique afin de garantir, notamment, la préservation du secret bancaire.

À cet égard, le groupe de travail souhaite souligner le silence, sur cette question, de l'accord bilatéral du 3 octobre 2019 entre les États-Unis et le Royaume-Uni sur le transfert de données dans le périmètre du *Cloud Act*[207]. Ce texte n'aborde, ni l'information des personnes directement visées par une demande de communication de preuves, ni celle des responsables des traitements dans lesquels se trouvent les informations demandées, alors même que le DOJ a sur ce sujet, soulignons-le, une position qui semble de bon sens[208].

Ce sujet mériterait d'être approfondi à l'occasion du règlement « e-evidence »[209], actuellement en débats devant le Parlement européen, afin qu'un principe de transparence, en évitant bien entendu tout risque d'entrave[210], soit clairement énoncé. Cette même demande vaut s'agissant du futur accord bilatéral entre l'Union européenne et les États-Unis, ce dernier étant également en cours d'examen devant la Commission.

---

[206] *§17. «The Agreement does not compel the CSP to remove encryption and is encryption neutral» - https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate.*

[207] *https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019?utm_source=b4d391f0-3d36-4077-8793-d5b2b06944c1&utm_medium=email&utm_campaign=govuk-notifications&utm_content=immediate.*

[208] *Cf. supra notes de bas de page 166 et 167.*

[209] *Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale COM/2018/225 final - 2018/0108 (COD).*

[210] *Cf. approche générale du Conseil du 30 novembre 2018, cf. article 11-1: « Confidentialité et information de l'utilisateur ». http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf*