DROIT DES MOYENS ET SERVICES DE PAIEMENT

LCB-FT : de la vérification d'identité à distance des personnes physiques



Pierre Storrer

Avocat au Barreau de Paris

Kramer Levin Naftalis & Frankel LLP

L'auteur invite les lecteurs à lui faire parvenir leurs réactions ou éléments d'actualité inédits : pstorrer@kramerlevin.com. Les propos de l'auteur n'engagent que celui-ci.

* Forum Fintech ACPR-AMF, Groupe de travail sur la vérification d'identité à distance des personnes physiques, Compt-rendu des travaux, 20 sept. 2019. Comp. ACPR, Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle, 14 déc. 2018, n°s 47 et s.

À propos des réflexions menées par un groupe de travail du Forum Fintech ACPR-AMF sur le sujet épineux de l'entrée en relation d'affaires à distance*.

INTÉRÊT ET ACTUALITÉ

C'est quasiment au quotidien que le juriste de banque, de paiements, d'assurances, etc., travaille aux conditions d'entrée en relation d'affaires avec les clients, relation le plus souvent nouée à distance dès lors qu'il s'agit de banques (ou d'assurances) en ligne ou de néobanques[1]. C'est presque tous les jours qu'il tente de concilier l'impossible : un parcours client fluide avec les exigences (qui sont autant d'obstacles) de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) ; avec, donc, l'impératif (catégorique) de la connaissance client (au titre de l'obligation de vigilance) ou KYC, selon le fameux acronyme, tellement fameux, d'ailleurs, qu'il tend à s'autonomiser de la LCB-FT elle-même[2].

La règle commune est connue : « *Avant d'entrer en relation d'affaires avec leur client ou de l'assister dans la préparation ou la réalisation d'une transaction* », les établissements assujettis doivent procéder en deux temps : ils « *identifient leur client et, le cas échéant, le bénéficiaire effectif* » et « *vérifient ces éléments d'identification sur présentation de tout document écrit à caractère probant* »[3]. Mais encore faut-il qu'ils « appliquent des mesures de vigilance complémentaires à l'égard de leur client », en particulier lorsque « *le client ou son représentant légal n'est pas physiquement présent aux fins de l'identification au moment de l'établissement de la relation d'affaires* »[4].

On prend dès lors connaissance avec grand intérêt du Compte rendu des travaux d'un groupe qui, réuni dans le cadre du Forum Fintech ACPR-AMF*, a réfléchi sur la vérification d'identité à distance des personnes physiques[5]. Ces travaux sont d'autant plus intéressants qu'ils pourraient « infuser » la transposition, en cours de finalisation, des dispositions de la 4e directive LCB-FT bis, censée intervenir d'ici au 10 janvier 2020[6]. Possibilité accrue dans la mesure où cette dernière modifie assez substantiellement le point a) de l'article 13 de la 4e directive [7] : alors que la rédaction d'origine prévoyait, sommairement, que les mesures de vigilance à l'égard de la clientèle comprennent, notamment, « *l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations obtenus d'une source fiable et indépendante* », la nouvelle dispose plus précisément que « *l'identification du client et la vérification de son identité, sur la base de documents, de données ou d'informations obtenus d'une source fiable et indépendante, y compris, le cas échéant, les moyens d'identification électronique et les services de confiance pertinents prévus par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil, ou tout*

[1] Cf., à ce sujet, ACPR, « Étude sur les modèles d'affaires des banques en ligne et des néobanques », *Analyses et Synthèses* n° 96, oct. 2018.

[2] On attend en effet régulièrement parler de KYC « et » de LCB-FT.

[3] CMF, art. L. 561-5, I. À quoi s'ajoute la prescription de l'article L. 561-5-1 : « *Avant d'entrer en relation d'affaires, les personnes mentionnées à l'article L. 561-2 recueillent les informations relatives à l'objet et à la nature de cette relation et tout autre élément d'information pertinent. Elles actualisent ces informations pendant toute la durée de la relation d'affaires.* »

[4] CMF, art. L. 561-10, 1°, auquel fait écho l'article R. 561-20.

[5] Précisons que le compte rendu de ce groupe de travail n'engage ni l'ACPR, ni l'AMF.

[6] Dir. (UE) 2018/843, 30 mai 2018, modifiant la directive (UE) 2015/849 sur la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.

[7] Dir. (UE) 2015/849, 20 mai 2015, relative à la prévention de l'utilisation du système financier aux fns du blanchiment de capitaux ou du financement du terrorisme.



autre processus d'identification sécurisé, électronique ou à distance, réglementé, reconnu, approuvé ou accepté par les autorités nationales concernées »[8]. L'occasion serait ainsi offerte de remodeler le texte de l'article R. 561-20 du CMF, objet de toutes les attentions, de celle du groupe de travail en particulier.

DE L'IDENTIFICATION ÉLECTRONIQUE

Là se trouve le nœud du problème ; là se noue toute l'ambiguïté, sinon l'incohérence, d'un nouveau droit français de la LCB-FT (issu de la transposition de la 4e directive LCB-FT, d'abord par l'ordonnance n° 2016-1635 du 1er décembre 2016 puis par le décret n° 2018-284 du 18 avril 2018)[9] qui, d'un côté, promeut l'identification électronique mais, de l'autre, ne s'en donne pas les moyens (ou, plutôt, à qui les moyens ne sont pas donnés).

Expliquons-nous : d'une part, le recours à un moyen d'identification électronique, au sens du règlement eIDAS[10], vaut – et vaut à lui seul, y compris en cas d'entrée en relation à distance – vérification de l'identité du client au sens du 2° du I de l'article L. 561-5 du CMF[11] ; mais, d'autre part, force est de constater que, de moyen d'identification électronique, il n'en existe pas et n'en existera pas, selon le groupe de travail réuni par le Forum Fintech, ni à court ni à moyen terme. Il n'en existe pas, du moins, au niveau élevé qui est requis. De sorte que l'on se trouve face à une réglementation « *mort-née* », ce qui est malheureux[12].

Il n'est qu'à consulter la liste des schémas nationaux d'identification eIDAS notifiés à la Commission européenne (*Overview of pre-notified and notified eID schemes under eIDAS*), on y trouve près d'une quinzaine de pays, à l'exception notable de la France. Pourquoi ?

[8] De même, alors que le point c) du 2) de l'annexe III de la 4e directive listait parmi les facteurs de risques les « *relations d'affaires ou transactions qui n'impliquent pas la présence physique des parties et qui ne sont pas assorties de certaines garanties telles qu'une signature électronique* », sa rédaction a été modifiée en : « *relations d'affaires ou transactions qui n'impliquent pas la présence physique des parties et qui ne sont pas assorties de certaines garanties telles que des moyens d'identification électronique, des services de confiance pertinents au sens du règlement (UE) n° 910/2014 ou tout autre processus d'identification sécurisé, électronique ou à distance, réglementé, reconnu, approuvé ou accepté par les autorités nationales concernées* ».

[9] Cf. P. Storrer, « Lutte antiblanchiment : l'avènement de la vérification d'identité au moyen de l'identification électronique », *Banque et Droit* n° 179, mai-juin 2018, p. 45.

[10] Règl. (UE) n° 910/2014, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

[11] Cf. CMF, art. R. 561-5-1 et R. 561-20. Comp. Rapport du Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB), Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France, sept. 2019, p. 85 : « *Le code monétaire et financier prescrit ainsi des mesures garantissant un haut niveau de sécurité pour qu'une identification à distance soit considérée équivalente à une identification en face-à-face. À défaut, l'identification à distance ne peut être possible qu'à condition qu'elle respecte des mesures complémentaires permettant d'assurer l'identification du client.* »

[12] Comp. ACPR, Étude sur les modèles d'affaires des banques en ligne et des néobanques, précit., p. 5, note 6 : « *Dans l'attente d'une identité numérique de niveau élevé en France, l'identification et la vérification de l'identité du client appellent des mesures de vigilance complémentaires. À partir du 1er octobre 2018, à la suite de l'entrée en application du décret n° 2018-284 du 18 avril 2018 renforçant le dispositif français de lutte contre le blanchiment de capitaux et le financement du terrorisme, un moyen d'identification électronique délivré dans le cadre d'un schéma français d'identification électronique de niveau de garantie élevé sera équivalent à la présentation de l'original d'un document officiel en cours de validité comportant sa photographie au regard des obligations relatives à la LCB-FT (futur article R. 561-5-1 du code monétaire et financier). Un tel schéma devra être au préalable notifié à la Commission européenne en application du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS).* »

Nous n'avons pas de réponse, sinon le constat suivant, fait par le groupe de travail : « *Si des moyens d'identification de niveau de garantie élevé sont disponibles dans d'autres pays européens, il n'est pas démontré que ceux-ci soient utilisés aux fins de la vérification d'identité par les établissements bancaires* » (p. 6). On est au moins certain, en France, que ces moyens ne sont pas utilisés puisqu'ils n'existent pas.

ÉTAT DES LIEUX

L'état des lieux de la vérification d'identité à distance doit donc débuter par ce constat en forme de carence : la seule mesure qui se suffirait à elle-même, en face-à-face comme à distance, n'est toujours pas disponible en France, sachant que le règlement eIDAS date toute de même de 2014... Si bien que nous sommes, les uns et les autres, obligés d'avoir recours à deux mesures de vigilance dites « *complémentaires* », parmi les six prévues à l'article R. 561-20 du CMF. C'est là qu'un deuxième constat s'impose, qui ajoute à la carence l'excès de zèle. Ne boudons pas notre plaisir à citer un peu longuement le Compte rendu du groupe de travail : « *Il semble que tous les pays n'aient pas fait le choix de donner une liste limitative de mesures de vigilance renforcées à appliquer pour les entrées en relation à distance. D'autres pays demandent des mesures de vigilance renforcées mais laissent les établissements financiers décider du contenu de ces mesures. Ce choix plus ouvert ne semble toutefois pas contraire aux objectifs de la 4e directive LCB-FT et des recommandations du GAFI. Plus généralement, les exigences françaises en matière de vérification d'identité pour une entrée en relation à distance seraient plus contraignantes que dans les autres pays européens, plaçant les établissements français dans une situation de "concurrence inégale" face aux établissements agissant sous le régime de la libre prestation de services* » (pp. 6-7)[13].

En mots choisis cela est dit, mais a le mérite de l'être. Quelles que soient ses raisons, la France en a trop fait et en fait trop en matière de vigilance, ce qui place nos opérateurs financiers dans une situation inégale, quand ce ne sont pas les opérateurs européens qui, passeportant sur notre sol par voie de libre établissement, se trouvent rattrapés par un droit français antiblanchiment largement « surjoué ». Souhaitons, en conséquence, à l'instar du RGPD, un règlement général LCB-FT plutôt qu'une énième directive aux transpositions erratiques[14] ; un texte d'application direct, donc, éventuellement accompagné d'un mécanisme de supervision européenne, ainsi qu'en ont appelé de leurs vœux, le 13 novembre dernier, certains ministres des finances[15]. L'état des lieux des mesures de vigilance complémentaires, dressé par le groupe de travail, conduit à ce dernier constat, somme toute accablant : des six mesures proposées par l'article R. 561-20, seules deux, voire trois, seraient praticables et, encore, selon des modalités (sécurité, protection des données, etc.) à préciser (cf. pp. 7-8). Sans compter que l'on apprend, finalement, que les moyens d'identification électronique de niveau élevé prônés par les 1° et 2° de l'article R. 561-5-1 (et valant aussi bien en face-à-face qu'à distance) se révéleraient inaccessibles aux établissements financiers et ne pourraient être développés que par la puissance publique (p. 10).

Le document sous commentaire s'achève par un certain nombre de propositions propres à remédier aux difficultés (c'est un euphémisme) évidentes de la vérification d'identité à distance des clients personnes physiques (on n'oubliera pas que cela n'est pas plus simple s'agissant des personnes morales). Celles-ci sont bien sûr intéressantes, mais encore de l'ordre du prospectif. On retiendra que le droit de la LCB-FT souffre peu ou prou du même mal que celui de l'authentification forte sous régime DSP 2 – dont on apprend que l'échéance de la migration a été reportée du 14 décembre de cette année au 31 décembre 2020[16] : la technologie tient la réglementation en l'état. Pour reprendre une observation figurant dans le dernier rapport annuel d'activité de Tracfin (2018) : « *La relation à distance est au cœur du paysage bancaire de demain. Des projets réglementaires et technologiques liés à l'identité numérique sont en discussion, et de nouveaux acteurs dits néobanques, agréés en France ou à l'étranger, apparaissent sur le marché français.* » (p. 14) Mais rien n'est encore prêt. ■

Achevé de rédiger le 13 novembre 2019.

[13] Comp. les orientations sur les facteurs de risque du Joint Committee of the European Supervisory Authorities, JC 2017 37, 4 janv. 2018, qui, fortes de 85 pages, sont autrement plus nuancées (trop d'ailleurs) que les mesures françaises.

[14] Cf. P. Storrer, « Pour un règlement général anti-blanchiment », *Revue Internationale du Patrimoine* n° 2, juin 2019, p. 21. Comp., depuis, *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, JC 2019 59, 4 oct. 2019, n° 36 : « *The ESAs consider that the EU's financial sector continues to be exposed to ML/TF risks because Member States have transposed EU law into national legislation in different ways.* »

[15] Cf. *Joint Position Paper by the Ministers of Finance of France, Germany, Italy, Latvia, the Netherlands and Spain, Towards a European Supervisory Mechanism for ML/FT*, p. 2 : « *This new supervision function should operate based on a set of harmonized, directly applicable rules.* »

[16] *Opinion of the European Banking Auhtority on the deadline for the migration to SCA for e-commerce card-based payment transactions*, EBA-Op-2019-11, 16 oct. 2019.