JANV. 2019

LA 5e DIRECTIVE LCB-FT[1].

Évolution ou Révolution ?

Alors que certains États membres de l'Union Européenne (UE) n'ont toujours pas transposé en droit national la 4e directive LCB-FT, Lutte Contre le Blanchiment et Financement du Terrorisme, le Parlement européen a adopté en date du 19 avril la proposition d'une nouvelle directive dite « 5e directive ».

Cette directive vise notamment à uniformiser la réglementation dans l'ensemble des pays de l'UE, renforcer la coopération entre les superviseurs et les institutions financières impactées par ce risque et adapter le dispositif LCB-FT existant à l'évolution des pratiques utilisées dans le blanchiment de capitaux et le financement du terrorisme (BC-FT).

La 4e directive LCB-FT transposée en France par l'ordonnance du 1er décembre 2016 est venue combler certains manquements de la 3e directive en instaurant notamment la création d'un registre de bénéficiaires effectifs, l'extension du champ d'application et de la notion de Personne Politiquement Exposée (PPE). La notion de PPE inclut depuis lors les cadres dirigeants des organisations internationales ainsi que les personnes qui exercent ou ont exercé des fonctions publiques importantes sur le territoire national. Ces principales évolutions ont engendré une mise à jour, par les entités assujetties, de leurs processus, avec l'instauration d'une analyse par les risques pour répondre à l'ensemble des attentes.

Des décrets sur la 4e directive continuent d'ailleurs à voir le jour comme le décret du 18 avril 2018 (précisant notamment la définition des « bénéficiaires effectifs », les mesures de vigilance à mettre en œuvre, les modalités de vérification de l'identité du client pour les relations d'affaires à distance ainsi que les procédures et le dispositif de contrôle interne nécessaires) et les récentes lignes directrices de l'ACPR et de TRACFIN[2].

Cependant, la diversité des nouveaux acteurs assurantiels et financiers, les récents scandales liés au blanchiment de capitaux ainsi que les craintes du législateur quant aux nouveaux moyens de financement du terrorisme, ont poussé le régulateur à établir une nouvelle directive : la 5e directive LCB-FT. Les 4e et 5e directives viennent donc compléter les dispositions de la 3e directive qui demeurent applicables.

L'objectif de cette publication est de comprendre les principales évolutions consacrées par la 5e directive et d'en saisir les impacts opérationnels qui en découlent.

Publication réalisée par
l'Expertise Center Enterprise Risk Management

R&D **6 EXPERTISE CENTERS AU SERVICE DES PRACTICES**

L'Expertise Center Enterprise Risk Management adresse l'ensemble des problématiques liées aux outils et méthodologies de gestion des risques, qu'ils soient actuels ou émergents, et analyse l'impact des évolutions normatives sur les contraintes en matière de conformité des acteurs assurantiels et bancaires, ainsi que des entreprises. Au travers des études et benchmarks réalisés, cet EC contribue au développement d'une vision critique et opérationnelle des pratiques de place, qui alimente la formation de nos consultants et nos communications.

[1] *LCB-FT : Lutte Contre le Blanchiment et le Financement du Terrorisme.*

[2] *Lignes Directrices conjointes de l'Autorité de contrôle prudentiel et de résolution et de TRACFIN sur les obligations de déclaration et d'information à TRACFIN, actualisées avec les mises à jours des dispositions législatives et règlementaire au 1er octobre 2018.*

Un manque d'uniformisation et de coopération au sein de l'Union européenne.

Le premier vecteur de réussite dans le déploiement d'une directive européenne repose sur la capacité et la volonté de chaque pays à la décliner et à l'appliquer au niveau national.

L'article 67 de la 4e directive LCB-FT exigeait donc en ce sens que l'ensemble des pays de l'UE aient transposé au 26 juin 2017 l'ensemble des mesures adéquates en matière de LCB-FT.

En se basant sur les travaux du GAFI (Groupe d'action Financière), il s'avère que cette exigence n'a pas été respectée et que certains pays tels que la Grèce, la Roumanie ou encore les Pays-Bas n'ont pas encore adapté leur droit interne aux exigences en matière de LCB-FT.

Révélateurs de cette hétérogénéité, les derniers scandales en matière de blanchiment de capitaux (Panama Papers, ABLV, Danske Bank) démontrent que ce manque d'uniformisation fragilise à la fois la sécurité sur le territoire mais également l'ensemble de la stabilité et la réputation du secteur financier européen.

L'enjeu repose sur la capacité des Cellules de Renseignement Financier (CRF) à lutter contre le risque BC-FT au niveau national mais aussi au niveau de l'UE. Sur ce dernier point, un travail reste à faire sur la coopération et la communication au sein de l'UE.

ACTUALITÉS

Le scandale Danske Bank
Septembre 2018

Révélateur d'un manque d'uniformisation au sein de l'UE.

Après le scandale de la banque lettone ABLV, la Danske Bank, première banque danoise, est soupçonnée d'avoir blanchi des milliards d'euros en provenance de Russie via sa filiale estonienne.

Ce nouvel évènement impliquant deux pays de l'UE et un « pays tiers équivalent » démontre les failles de la réglementation actuelle, trop hétérogène au sein des pays de l'UE.

FOCUS

Le Panama Paper

Pour rappel, le scandale des Panama Papers a éclaté en avril 2016 et représente la plus grande fraude fiscale de l'histoire du XXIe siècle. Ce scandale a été révélé par l'intermédiaire d'un lanceur d'alerte anonyme qui a fourni plus de 11,5 millions de fichiers à des journalistes pour dénoncer la création de société *offshores* notamment utilisées à des fins d'évasion fiscale ou de blanchiment d'argent.

Liste des principales défaillances organisationnelles.

La 5e directive permet de compléter le dispositif existant et de remédier aux carences constatées de la 4e directive tels que :

- le manque de contrôle des transactions émises ou reçues par des pays tiers à haut risque ;
- le manque de contrôle sur les transactions effectuées en monnaie virtuelle ;
- le manque de mesures relatives au contrôle des instruments prépayés anonymes (cartes bancaires prépayées, fiduciaires, etc.) ;
- les restrictions d'accessibilité des CRF aux informations relatives des titulaires de comptes bancaires, comptes de paiement ;
- le manque d'homogénéisation au sein de l'UE.

La 5e directive : principales mesures et enjeux opérationnels.

Les 4 principales mesures* :

Champ d'application

Élargissement du *scope* des acteurs assujettis aux obligations de LCB-FT aux acteurs du « marché des crypto-monnaies ».

Pays tiers à risque

Renforcement des mesures à l'égard des clients établis dans ces pays.

Coopération & Supervision

Amélioration de la supervision consolidée des groupes au sein de l'UE, renforcement de la coopération entre l'ensemble des superviseurs LCB-FT et généralisation des registres centraux de comptes bancaires.

Identification numérique

Utilisation de l'identification numérique prévue par le règlement eIDAS[1] (*Electronical IDentification And trust Services*) dans le cadre de l'entrée en relation à distance avec le client.

* : détaillées dans cette publication.

Champ d'application.

Problématique et réponse de la 5e directive

Afin d'adapter le dispositif LCB-FT européen aux nouvelles pratiques utilisées dans le blanchiment de capitaux et le financement du terrorisme, le champ d'application a été élargi aux acteurs du crypto-marché : fournisseurs de services de change et fournisseurs de portefeuilles.

L'utilisation des cryptos-actifs tels que le Bitcoin (crypto-monnaie semi-anonyme) ou le Moreno (crypto-monnaie anonyme) par les cybercriminels et les terroristes a terni la réputation de ce marché et a poussé le législateur européen à l'intégrer dans le *scope* de la LCB-FT. Pour rappel, les cryptos-actifs sont des instruments numériques se servant d'un réseau informatique et reposant sur la technologie de *Blockchain*, particulièrement adaptée à la certification d'informations entre parties et donc, par extension, aux transactions financières.

Si la technologie utilisée est reconnue pour les gains d'efficacité potentiels engendrés, l'avancée technologique ou encore l'enregistrement des transactions au sein d'un registre, les risques qu'elle engendre restent cependant significatifs. Il est important de rappeler que les plateformes de cryptos-actifs permettent d'échanger des monnaies non réglementées décentralisées contre des monnaies à cours forcé (euros, dollars, etc.), mais ce n'est pas le seul risque majeur identifié. En effet, le degré d'anonymat, l'opacité du système ou encore la complexité de cette technologie rendent difficile le contrôle de ce marché et fragilise par la même le niveau de confiance de l'UE et des autorités de contrôle.

Intégration des acteurs du crypto-marché : enjeux de la mesure

Les manquements notables tant en matière de connaissance client (KYC, pour *Know Your Customer*) que de surveillance constante des opérations auxquels s'ajoute l'utilisation de crypto-monnaies anonymes ou semi-anonymes facilitent l'utilisation de la *Blockchain* à des fins de blanchiment de capitaux ou de financement du terrorisme. Les plateformes telles que Binance, Coinbase, BitPanda ou encore Yobit seront donc désormais concernées par la mise en place d'un dispositif de lutte contre le blanchiment et le financement du terrorisme.
Si les acteurs du crypto-marché disposent d'un délai pour se mettre en conformité de par le délai légal de transposition en droit français, ils seront désormais bien assujettis à la réglementation. La mise en place de leur dispositif devra prendre en compte l'ensemble de la réglementation LCB-FT (que ce soit la 3e, 4e ou 5e directive), les mesures de gel des avoirs mais aussi le KYC. Du côté des institutions financières, notamment des banques de détail, les mesures de vigilance doivent être renforcées au maximum lorsque des fonds semblent provenir du marché des crypto-actifs, tant que des dispositifs efficients de lutte contre le BC-FT n'auront pas été mis en place sur ce marché.

[1] *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.*

Coopération & Supervision.

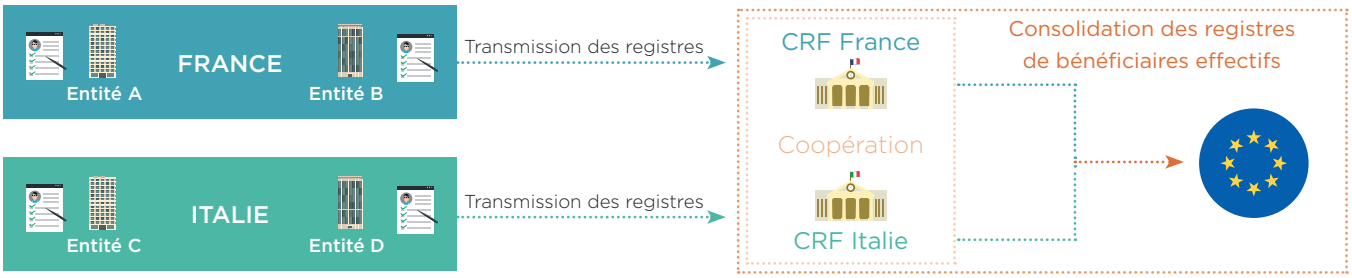
Alors que la 4e directive avait introduit l'obligation de signaler les bénéficiaires effectifs, sa révision vient renforcer d'avantage ce nouveau cadre. Les États membres auront dorénavant l'obligation de communiquer le registre des bénéficiaires effectifs de « type commercial », (à savoir les personnes morales) à l'ensemble du public, sans restriction d'accès. Ces informations devront être mises à jour régulièrement et les entités assujetties devront appliquer leur obligation de vigilance, telles que revues par les textes du code monétaire et financier issus de la 3e directive LCB-FT aussi bien sur leurs nouveaux clients qu'à l'égard de leurs clients existants, selon l'appréciation du niveau des risques.

Concernant les bénéficiaires effectifs des *trusts/fiducies* ces derniers devront être enregistrés à l'endroit où le *trustee/fiduciaire* réside et devront être partagé avec les autres États Membres pour permettre d'éviter une multiplication des bénéficiaires effectifs identiques.

Par ailleurs, la communication sur le registre de ces bénéficiaires effectifs de *trusts/fiducies*, ne pourra être accessible qu'aux personnes ayant démontré un intérêt légitime à cet accès. Autrement dit, qui seront autorisées par ordonnance du juge commis à la surveillance du Registre du Commerce et des Sociétés (RCS) auprès duquel est immatriculée la société. Pour ce faire, les tiers devront communiquer une requête au greffe du tribunal de commerce. Cette dernière devra préciser l'objet et le fondement de la requête, ainsi que l'indication des pièces sur lesquelles elle est fondée.

Les entreprises assujetties devront donc s'assurer que leur registre de bénéficiaires effectif est communiqué aux CRF et consolidé entre les différentes entités d'un même groupe. Des contrôles devront être mis en place afin de s'assurer de la mise à jour à fréquence régulière de leurs registres

Pour rappel, en ce qui concerne la France, le décret du 18 avril 2018 prévoyait déjà l'intégration de cette mesure.



RAPPEL

Décision n°2016-591 QPC* du Conseil constitutionnel
21 octobre 2016

Pour rappel, le 21 octobre 2016, le Conseil Constitutionnel avait censuré le registre des bénéficiaires effectifs de *trust/fiducie* en considérant que l'obligation de lutte contre le blanchiment et le financement du terrorisme ne pouvait justifier l'atteinte à la vie privée qu'engendrait une communication publique et sans restriction d'accès dudit registre. Les nouvelles mesures d'accessibilité au registre prises par la 5e directive, devront permettre au Conseil constitutionnel de valider, cette fois-ci, la création du registre des bénéficiaires effectifs de *trust* et leur communication.

* QPC : Question prioritaire de constitutionnalité.

L'identification numérique.

Renforcement de la légitimité de l'identification numérique

Dans le cadre des relations d'affaires à distance, la 5e directive intègre l'utilisation de l'identification numérique telle que définie par le règlement eIDAS.

Le marché de la confiance numérique a été décrit dans la communication de la Commission « Stratégie pour un marché unique numérique en Europe » et prévu dans le règlement eIDAS permettant ainsi de faire valoir cette identification numérique comme sécurisée et sûre, au même titre qu'une entrée en relation « face à face ».

La réglementation actuelle définit la relation d'affaire à distance comme risquée en matière de risque de BC-FT. Cette nouvelle mesure vient donc alléger les exigences pour les institutions financières n'ayant que des relations d'affaires à distance mais nécessite un remaniement de leur dispositif interne.

eIDAS : opportunité ou contrainte

L'intégration des mesures prévues par le règlement eIDAS au sein de l'entreprise a un impact opérationnel conséquent sur le dispositif LCB-FT. L'intégration des mesures eIDAS va permettre aux institutions financières ayant axés leurs stratégies sur le développement commercial à distance avec leurs clients de réduire le niveau de vigilance requis et donc de revoir la classification des risques LCB-FT.
Si la plus grande partie du marché a déjà intégré la signature électronique dans ses processus, un travail reste à faire sur l'homogénéisation et la conformité du dispositif en place.

CE QU'IL FAUT SAVOIR SUR L'eIDAS

- **Adoption :** le 23 juillet 2014 par le Parlement européen et le Conseil de l'UE pour une application au 1er juillet 2016.
- **Champ d'application :** Il concerne les organismes du secteur public et les prestataires de services de confiance tels que les assureurs.
- **Objectif :** promouvoir le développement d'un marché de la confiance numérique reposant sur l'homogénéité, la confiance et la sécurité.
- **Autorité compétente en France :** l'ANSSI en tant que garante de la sécurité pour l' « identification numérique » et organe de contrôle pour les « services de confiance ».

Les pays tiers à haut risque.

La proposition de directive du Parlement et du Conseil modifiant la 4e directive avait fait état de l'importance de limiter les relations d'affaires ou les transactions impliquant des pays tiers à haut risque, dont les obligations de LCB-FT ne correspondraient pas aux exigences fixées par l'UE mais également par le GAFI. En effet, ces pays présentent des carences stratégiques en matière de LCB-FT qui font peser une menace significative sur le système financier de l'UE.

L'objectif de cette mesure est de limiter au maximum le risque de voir « une chasse à la législation la moins stricte s'opérer à l'égard des pays tiers à haut risque ». Désormais, l'ensemble des entités assujetties devront obligatoirement obtenir des informations supplémentaires sur les bénéficiaires effectifs, les clients, l'origine des fonds ou du patrimoine mais l'autorisation d'entrer en relation ou de poursuivre une relation d'affaire sera également dépendante d'un niveau de hiérarchie plus élevé dans les entreprises (tels que les Dirigeants).

À cela s'ajoute l'obligation pour les États membres d'exiger, lors de la transposition de la directive, la mise en place de mesures complémentaires de vigilance renforcées à l'égard de la clientèle avec a *minima* :

- la mise en place des mécanismes de déclaration renforcés ou une déclaration systématique des transactions financières ;
- la limitation des relations d'affaires ou des transactions avec des personnes physiques ou des entités juridiques provenant de pays tiers recensés comme étant des pays à haut risque ;
- le refus d'établissement de succursales ou filiales provenant de pays non dotés de dispositif suffisant.

De nouvelles procédures devront donc être mises en place aussi bien concernant l'obtention des informations auprès des bénéficiaires effectifs que sur le niveau de validation des relations d'affaires ou transactions qui impliqueraient des pays tiers à haut risque.

À cela devra s'ajouter la mise en place de contrôles pour s'assurer de la mise à jour régulière des informations.

ACTUALITÉS

La liste noire européenne

Depuis juillet 2016, la Commission européenne établi une liste noire des pays tiers à haut risque, commune à l'ensemble des pays de l'UE.

Cette liste est mise à jour régulièrement et a été modifiée pour la dernière fois le 6 mars 2018 par le Règlement délégué et comprend à titre d'exemple la Syrie, la Corée du Nord ou encore le Laos.

Des mesures de vigilance renforcées doivent être appliquées dans les relations avec les clients établis dans ces pays.

La commission européenne travaille actuellement sur une liste noire plus indépendante et la plus exhaustive possible en incluant d'autres critères que ceux habituellement retenus par le GAFI.

Conclusion.

Le projet de 5e directive n'est donc pas une révolution mais élargit le champ d'application des obligations en réponse aux évolutions du marché et des techniques de BC-FT toujours plus complexes, en ciblant une protection efficace de l'intégrité et du bon fonctionnement du système financier.

De par ces exigences toujours plus contraignantes, les institutions financières doivent s'adapter et évoluer dans leurs approches de gestion des contraintes règlementaires et législatives. Un fort investissement financier y est consacré et la réduction du coût de ces investissements est donc un levier intéressant pour accroître les marges de rentabilité.

Pour répondre à ces évolutions, les Regtechs sont apparues dans le paysage financier et se concentrent sur l'amélioration des systèmes de conformité et de contrôle interne des institutions financières. Leur objectif est d'avoir une approche agile, faciliter les rapports règlementaires et développer l'automatisation pour s'adapter aux obligations en matière de conformité règlementaire.

En parallèle, les banques et autres sociétés de services financiers ont déjà adopté l'automatisation des processus métier à travers les dernières avancées informatiques, telles que l'utilisation des *Big Data* et la robotisation, ou encore l'intégration de l'intelligence artificielle (IA). Nul doute que cela permettra, encore une fois, une nette amélioration de la qualité de la détection et de l'analyse via des approches hybrides s'appuyant sur la combinaison de plateforme *Big data* (ex : Hadoop) et d'outils spécialisés (ex : RPA).

optimind.
manage risk, build your future

Société de conseil indépendante, Optimind accompagne les organismes assureurs, banques et grandes entreprises dans le ciblage des opportunités de nature à accroitre leurs performances. Nous apportons du conseil et des solutions pour répondre aux défis majeurs de la compétitivité, de la transformation et de la réglementation. Ces enjeux, malgré les risques, offrent des opportunités de développement considérables.
Nos lignes de services couvrent chaque maillon de la chaîne de valeurs de nos clients : Strategy, Finance, Risk, Compliance, Market, Human Resources, Digital Transformation, Data, BPO.

optimind.com

Strategy
Finance
Risk
Compliance
Human resources
Digital transformation
Market
DATA
Business Process Outsourcing

Contacts.

Practice Risk Management

Dan Chelly - Senior Partner - dan.chelly@optimind.com

Alain Le Corre - Partner - alain.lecorre@optimind.com

Presse

Marine de Pallières - Communication & Public Relations Manager - marine.depallieres@optimind.com

Optimind SAS au capital de 400 950 euros, 46 rue La Boétie - 75008 PARIS. Siret : 418 861969 00099 - Code APE : 7022Z.

Les documents d'Optimind sont produits selon des processus respectueux de l'environnement. Ils sont imprimés par un prestataire certifié Imprim' Vert®, sur des papiers certifiés par des labels de qualité environnementaux. Conception réalisation : OptiComRH. Crédits photos : Shutterstock, iStock.