

CHAPITRE 3
–
SÉCURITÉ FINANCIÈRE : LA
RÉGLEMENTATION
POUR LA LUTTE
CONTRE LE BLANCHIMENT
ET LE FINANCEMENT
DU TERRORISME

INTRODUCTION

Selon de récentes estimations de l'Organisation des Nations unies (ONU), les produits d'activités criminelles blanchis chaque année représentent entre 2 % et 5 % du PIB mondial, soit 1 600 à 4 000 milliards de dollars par an. Dans ce contexte, la mise en place de dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme est apparue indispensable et les organismes financiers sont au cœur de cette lutte dans le cadre d'une réglementation répondant aux recommandations du Groupe d'action financière et aux directives européennes.

Ce chapitre aborde le cadre juridique et institutionnel de la lutte contre le blanchiment et le financement du terrorisme et explicite les mécanismes du blanchiment.

Quant à la corruption, elle absorbe chaque année 2 % de la richesse mondiale (source : FMI, 2016). À eux seuls, les pots-de-vin versés chaque année dans le monde sont évalués entre 1 500 à 2 000 milliards de dollars, soit presque le produit intérieur brut (PIB) français à cette date. Ce chapitre détaille notamment les obligations en matière de lutte contre la corruption, les échanges automatiques d'information et la gestion des embargos.

Enfin il précise les sanctions encourues selon les différents types d'infractions.

SOMMAIRE DU CHAPITRE

I	DÉFINITIONS, LE PROCESSUS DE BLANCHIMENT, LE CADRE INSTITUTIONNEL, LES OBLIGATIONS, LES SANCTIONS	119
	1. les formes du blanchiment de capitaux et du financement du terrorisme	119
	2. Le cadre juridique et réglementaire	120
	3. L'obligation d'identifier le client.....	123
	4. L'obligation de vigilance	125
	5. Cas particulier des « personnes politiquement exposées »	127
	6. L'obligation de détecter les opérations suspectes	128
	7. Le rôle de Tracfin.....	130
	8. Les implications d'organisation dans les établissements financiers	133
	9. Les risques de sanction.....	135
	10. Les régimes de sanctions économiques et financières.....	135
	11. L'échange automatique et obligatoire dans le domaine fiscal	137
	12. Le dispositif FATCA (<i>Foreign account tax compliance act</i>)	137
	13. La lutte contre la corruption.....	138
	Pour aller plus loin	140

DÉFINITIONS, LE PROCESSUS DE BLANCHIMENT, LE CADRE INSTITUTIONNEL, LES OBLIGATIONS, LES SANCTIONS

1. LES FORMES DU BLANCHIMENT DE CAPITAUX ET DU FINANCEMENT DU TERRORISME

1.1. Définition du blanchiment de capitaux

Le blanchiment de capitaux est un délit consistant à rendre licites des fonds issus de la délinquance pour dissimuler la provenance des profits et obtenir l'usage du placement de ces fonds.



Code pénal (article 324-1)

Le blanchiment est « *le fait de faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect.*

Constitue également un blanchiment le fait d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit. »

Le délit de blanchiment est qualifié d'« aggravé » :

- lorsqu'il est commis de façon habituelle ou en utilisant les facilités que procure l'exercice d'une activité professionnelle ;
- ou lorsqu'il est commis en bande organisée.

Le **blanchiment de capitaux** recouvre :

- **la conversion ou le transfert des biens, dont l'auteur sait** qu'ils sont le **produit d'un délit ou d'un crime, dans le but de dissimuler ou de déguiser l'origine illicite des biens** ou d'aider toute personne impliquée dans l'infraction principale à échapper aux conséquences de ses actes ;
- **l'acquisition, la détention ou l'utilisation des biens par une personne qui sait**, lors de leur réception, que ces **biens constituent le produit d'un crime** ;
- **la participation à l'une des infractions** établies ou à toute autre association, entente, tentative ou complicité par fourniture d'une assistance, d'une aide ou de conseils.



Code pénal (article 324-1-1)

Le législateur a introduit une présomption d'« argent sale ».

« *Les biens ou les revenus sont présumés être le produit direct ou indirect d'un crime ou d'un délit dès lors que les conditions matérielles, juridiques ou financières de l'opération de placement, de dissimulation ou de conversion ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de ces biens ou revenus.* »

1.2. Le financement du terrorisme

Financer le terrorisme consiste pour une personne ou une entité à fournir ou à réunir des fonds dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés pour commettre un acte terroriste.

Le **financement du terrorisme** est souvent **difficile à déceler dans la surveillance des flux financiers**. En effet, les sommes en circulation peuvent être de faible montant et les terroristes peuvent utiliser des structures légales (dons, organismes caritatifs, associations etc.) pour « noircir » des fonds souvent d'origine licite.

1.3. Le processus de blanchiment de capitaux

Il s'agit pour le criminel d'utiliser un circuit financier et des produits d'investissement pour conférer une légalité apparente à de l'argent en provenance d'une activité criminelle.

Avant 2009, les soupçons portaient sur de l'argent sale provenant d'activités précises (trafics de stupéfiants, criminalité organisée...).

Depuis 2009, l'argent provenant de tout crime ou délit punissable d'au moins un an d'emprisonnement doit faire l'objet d'une déclaration de soupçon.

Les infractions visées ont alors couvert un périmètre plus large, par exemple ; travail dissimulé, escroquerie, abus de confiance et abus de faiblesse, abus de biens sociaux, vol, recel, contrefaçon, corruption...).

La fraude fiscale n'est prise en considération qu'en présence d'au moins l'un des **seize critères** définis par décret, comme par exemple : des comptes de passages, des opérations dont l'objet économique est incohérent, des opérations immobilières manifestement sous-évaluées ou des allers-retours de fonds avec des pays étrangers sans motif cohérent.

Le blanchiment de capitaux s'opère en **3 étapes**.

- **Le placement** consiste à introduire dans le système financier des sommes d'origine douteuse (dépôt d'espèces...). *C'est l'étape la plus visible.*
- **La dissimulation (ou empilement)** consiste à éloigner les fonds de leur source, par une série de transformations et de placements : virements, transferts, montages anormalement complexes, etc. *Ces opérations se font en l'absence de raison économique valable et tangible.*
- **La conversion (ou intégration)** est le procédé consistant à réintroduire les fonds dissimulés dans des activités économiques légitimes : immobilier, placements financiers, acquisition d'entreprises, etc. À ce stade, seules les caractéristiques du bénéficiaire de l'opération peuvent permettre de suspecter l'origine douteuse des fonds.

2. LE CADRE JURIDIQUE ET RÉGLEMENTAIRE

2.1. Le contexte réglementaire

En France, depuis la première loi en juillet 1990 relative à la participation des organismes financiers à la lutte contre le blanchiment des capitaux provenant du trafic des stupéfiants, de nombreux textes législatifs et réglementaires ont renforcé la lutte contre le blanchiment en étendant son champ d'application et en précisant les attentes des autorités vis-à-vis de ces organismes.

Le dispositif actuel est issu de la transposition de directives européennes successives.

La lutte contre le blanchiment de capitaux et le financement du terrorisme est désignée la plupart du temps par les acronymes LCB-FT, parfois par LBC-FT ou par LAB-FT (en anglais : AML/CTF).

En juin 2016, la Commission européenne a proposé une modification de la 4^e directive anti-blanchiment dans le cadre de son plan d'action de lutte contre le financement du terrorisme.

Les apports de la 5^e directive anti-blanchiment publiée le 19 juin 2018 au Journal officiel de l'Union européenne ont été transposés dans le droit français par ordonnance et décret du 12 février 2020. La cinquième directive vient compléter les dispositions de la quatrième directive, qui demeure applicable. Elle rationalise le dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme tout en assouplissant certaines dispositions

Les principales nouveautés de la 5^e directive sont les suivantes :

- **élargissement du champ des activités assujetties** notamment les activités de conseil fiscal et certains prestataires de services liés aux actifs numériques (crypto-actifs) ;
- **renforcement des obligations de transparence** relatives aux **bénéficiaires effectifs des sociétés et des trusts / fiducies** : obligation pour les sociétés d'obtenir et conserver des informations sur leur bénéficiaire effectif et sanction en cas de non-transmission de l'information aux assujettis dans le cadre des mesures de vigilance, accès aux registres élargis, etc. ;

- **abaissement des seuils au-delà desquels des mesures LCB-FT doivent être conduites** pour les transactions en **monnaie électronique** ;
- la mise en place de moyens d'identification électronique ou à distance sécurisés et de vérification des données prévus par le Règlement européen eIDAS sur l'identification électronique ;
- application de **mesures de vigilance renforcées pour les relations d'affaires ou transactions** impliquant des **pays tiers à haut risque** ;
- **mécanisme de supervision consolidée du dispositif de LCB-FT à l'échelle des groupes bancaires et d'assurance.**

La 5^e directive a aussi créé des listes des « fonctions publiques importantes » pour surveiller les personnes politiquement exposées (PPE) et a élargi le champ des assujettis (les agents immobiliers).

La Directive 2018/1673 du 23 octobre 2018⁵² établit des règles minimales concernant la définition des infractions et sanctions pénales dans le domaine du blanchiment de capitaux, Elle comporte une liste harmonisée sur le plan européen de **vingt-deux infractions constitutives du blanchiment d'argent** incluant notamment la **cybercriminalité**. Elle élargit le champ d'application à la complicité d'actes de blanchiment, étend la responsabilité pénale aux personnes morales et alourdit également les sanctions.

2.2. Les principes du dispositif actuel

Le dispositif actuel repose sur les **grands principes suivants** :

- **l'identification et la connaissance** actualisée des clients et des bénéficiaires effectifs ;
- **l'approche graduée par les risques**, qui détermine le niveau de vigilance adapté au profil de risque du client :
 - elle exige **une vigilance constante** sur le client et sur ses opérations, lors de l'entrée en relation et tout au long de la relation d'affaires,
 - et **la modulation de ces obligations** en fonction du risque ;
- **la détection et le traitement des opérations inhabituelles ou suspectes** et, le cas échéant, à partir de l'utilisation d'outils informatisés mis en place à cette fin ;
- **l'obligation de déclaration en cas de soupçon** et de transmission d'informations à la cellule de renseignement financier Tracfin dans le respect de la confidentialité ;
- la faculté, pour les responsables de la lutte contre le blanchiment de capitaux et le financement du terrorisme, d'échanger des informations sous certaines conditions ;
- la mise en place de procédures de contrôle interne dédiées et de formations adaptées au personnel.

2.3. Les principaux acteurs en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

2.3.1. Au niveau international

L'Organisation des Nations unies (ONU) , le Comité de Bâle, le GAFI, Moneyval⁵³, l'Autorité bancaire européenne (ABE ou EBA) et diverses autres institutions publiques ou privées⁵⁴ participent à l'élaboration des principes fondamentaux de la lutte contre le blanchiment et le financement du terrorisme.

Le Groupe d'action financière sur le blanchiment de capitaux (GAFI, en anglais FATF est un organisme intergouvernemental dont l'objectif est d'émettre des recommandations aux États en matière de LCB-FT. Périodiquement, le GAFI évalue les dispositifs de LCB-FT mis en œuvre par les États et territoires et rend compte des progrès réalisés en la matière.

⁵² La Directive (UE) 2018/1673 du Parlement européen et du Conseil du 23 octobre 2018 visant à lutter contre le blanchiment de capitaux au moyen du droit pénal est parfois dénommée improprement « 6^e directive ».

⁵³ Moneyval ou Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme est un organe de suivi permanent du Conseil de l'Europe. Il évalue la conformité aux principales normes internationales en matière de lutte contre le blanchiment des capitaux et contre le financement du terrorisme et évalue l'efficacité de l'application de ces normes. Il peut émettre des recommandations aux autorités nationales quant à des améliorations nécessaires de leurs systèmes.

⁵⁴ Notamment le Groupe Egmont regroupant les cellules de renseignement financier telles que Tracfin ou le Wolfsberg Group, association de treize grands groupes bancaires internationaux.

Le GAFI publie plusieurs fois par an des listes actualisées :

- liste des juridictions à l'encontre desquelles le GAFI appelle à appliquer des contre-mesures (couramment appelée « liste noire ») ;
- liste des juridictions présentant des défaillances stratégiques en matière de LCB-FT et qui sont soumises à un processus de surveillance (couramment appelée « liste grise »).

2.3.2. Au niveau européen

La réglementation applicable en France est issue des directives européennes.

Un règlement délégué de la Commission européenne recense les pays tiers à haut risque présentant des carences stratégiques en matière de LCB-FT. La liste de ces pays est actualisée régulièrement.

2.3.3. En France

Pour s'assurer de la bonne application de ces textes, des autorités de tutelle ou des ordres ou organisations professionnels interviennent pour fixer la doctrine ou pour exercer un contrôle.

Les autorités de tutelle suivantes sont chargées de la surveillance des organismes financiers (voir leurs rôles dans le Chapitre 1, *Le cadre de tutelle français*) :

- l'Autorité de contrôle prudentiel et de résolution (ACPR) ;
- l'Autorité des marchés financiers (AMF).

Par ailleurs, des sanctions professionnelles peuvent être prononcées par :

- la Commission des sanctions de l'ACPR ;
- la Commission des sanctions de l'AMF ;
- la Commission nationale des sanctions.

Des acteurs institutionnels interviennent également dans la lutte contre le blanchiment de capitaux et le financement du terrorisme :

- Tracfin (voir le paragraphe 7 ci-après) ;
- les autorités policières et judiciaires ;
- le procureur de la République.

Le dispositif de LCB-FT s'appuie sur la coopération de professionnels qui sont en mesure de détecter les flux financiers de blanchiment des capitaux et de financement de terrorisme.

Les professions assujetties à la réglementation de LCB-FT sont notamment les suivantes :

- les **entités des secteurs bancaire et financier** : instituts d'émission, **établissements de crédit**, établissements de monnaie électronique, établissements de paiement, sociétés de financement, **entreprises d'investissements**, **sociétés de gestion**, **conseillers en investissements financiers**, intermédiaires en financement participatif, **assureurs**, **courtiers en assurances**, changeurs manuels et établissements équivalents ou succursales établis au sein de l'Union européenne ;
- les **intermédiaires immobiliers** ;
- les **professions du chiffre et du droit** (experts comptables, commissaires aux comptes, avocats, notaires, huissiers de justice, mandataires de justice - administrateurs judiciaires et mandataires judiciaires) ;
- les **entités du secteur des jeux** ;
- les **négociants en biens et services de grande valeur** (pierres précieuses, matériaux précieux, antiquités ou œuvres d'art, etc.) ;
- et les **sociétés de domiciliation**.

3. L'OBLIGATION D'IDENTIFIER LE CLIENT

3.1. La notion de relation d'affaires

Une relation d'affaires est nouée lorsqu'une personne engage une relation professionnelle ou commerciale qui est censée s'inscrire dans une certaine durée.

La notion de relation d'affaires fait référence non seulement aux clients, mais également à toute personne avec qui l'organisme financier peut s'engager dans une relation contractuelle (banquier, distributeur, prestataire de services, fournisseurs...).

Les règles d'identification et de vigilance en matière de LCB-FT s'appliquent également aux « clients occasionnels », moyennant des dispositions particulières et selon le montant des capitaux engagées.

3.2. L'obligation d'identification et de connaissance du client avant l'entrée en relation

Tout établissement doit s'assurer de **l'identité de tout nouveau client** (particulier ou personne morale) et recueillir des informations sur **l'objet et la nature** de la relation d'affaires :

- il identifie le client et, le cas échéant, le bénéficiaire effectif ;
- il vérifie l'identité du client et constitue un dossier avec des **justificatifs écrits probants** ;
- il s'enquiert de **tout élément d'information** pertinent sur l'objet de la relation d'affaires.



Zoom

L'identification d'un client s'effectue :

- pour un client personne physique : par la présentation d'un document officiel d'identité en cours de validité ou par moyen d'identification électronique ;
- pour un client personne morale : par la présentation de l'original ou de la copie de tout acte ou extrait de registre officiel datant de moins de 3 mois ou extrait de Journal officiel.

L'établissement, au vu de ces éléments, pourra alors déterminer le profil risque LCB-FT de son client et ainsi vérifier la cohérence des opérations qui seront réalisées par la suite.

À défaut d'identifier le client et, le cas échéant, son bénéficiaire effectif et/ou d'obtenir les informations relatives à l'objet et à la nature de la future relation d'affaires, l'établissement n'ouvre pas le compte et n'établit ni ne poursuit aucune relation d'affaires avec ce client.

3.3. L'actualisation de la connaissance du client

Lorsque l'établissement a de bonnes raisons de penser que l'identité de son client et les éléments d'identification précédemment obtenus ne sont plus exacts ou pertinents, il procède à nouveau à l'identification du client et à la vérification de son identité et, le cas échéant, à l'identification et à la vérification de l'identité de son bénéficiaire effectif.

Pendant toute la durée de la relation d'affaires, l'établissement recueille, met à jour et analyse les éléments d'information qui permettent de conserver une connaissance appropriée de ses relations d'affaires.

La nature et l'étendue des informations collectées, ainsi que la fréquence de la mise à jour de ces informations et l'étendue des analyses menées sont adaptés au risque de blanchiment des capitaux et de financement du terrorisme présenté par la relation d'affaires.

3.4. La recherche du bénéficiaire effectif

L'identification du bénéficiaire effectif a pour principal objectif d'empêcher l'utilisation illicite de constructions juridiques par les blanchisseurs de capitaux et les financeurs du terrorisme. En effet, derrière une structure peuvent se cacher un ou plusieurs bénéficiaires effectifs. Des empilements de structures « écran » peuvent dissimuler un ou plusieurs bénéficiaires effectifs derrière une « chaîne de détention ».

3.4.1. Définition

Le bénéficiaire effectif est la ou les personnes physiques :

- soit **qui contrôle(nt), directement ou indirectement**, le client personne morale ou construction juridique de type fiducie ou trust ;
- soit **pour laquelle (lesquelles) une opération est exécutée ou une activité réalisée**.

Lorsque le client, personne physique, agit pour son compte propre, il est le bénéficiaire final et réel de l'opération. Dans ce cas, il n'y a pas de bénéficiaire effectif distinct.

En revanche, la procédure d'identification d'une personne morale est étendue à l'identification du bénéficiaire effectif de celle-ci.

3.4.2. Identification du bénéficiaire effectif d'une personne morale

Le bénéficiaire effectif d'un établissement financier qui effectue une opération pour le compte de son client, n'est pas le client final mais la personne physique qui contrôle l'établissement financier.

Le bénéficiaire effectif d'un client personne morale ou entité est la personne physique :

- **qui détient, directement ou indirectement, plus de 25 % du capital, des droits de vote ou des droits sociaux ;**
- **qui, à défaut et en dernier ressort, représente légalement la société.**

Le législateur a fixé des critères permettant de caractériser les bénéficiaires effectifs selon que le client est une société, un OPC ou une construction juridique d'un autre type.

Dans le cas d'une chaîne de détention, le professionnel assujéti doit rechercher les personnes physiques présentes à chacun des niveaux de la chaîne et s'attacher pour chacune d'elles à calculer les pourcentages de détention du capital ou des droits de vote du client.

Le professionnel assujéti a, au regard de la réglementation, une obligation de moyens et doit justifier auprès des autorités des diligences qu'il a mises en œuvre pour identifier le bénéficiaire effectif.

Sauf situation de risque de blanchiment élevé, et en l'absence de tout soupçon, le professionnel assujéti peut vérifier l'identité du bénéficiaire effectif des personnes morales et entités figurant dans le registre des bénéficiaires effectifs tenu par le Greffe du Tribunal de Commerce et, le cas échéant, le registre étranger tenu par l'autorité publique, en collectant un extrait du registre.

Une vigilance constante doit être observée sur l'identité du bénéficiaire. Le professionnel doit adapter son niveau de vigilance au risque présenté par le bénéficiaire effectif.

3.5. La tierce introduction

3.5.1. Définition

La tierce introduction est une relation entre établissement assujéti et un tiers introducteur, par laquelle l'établissement confie au tiers introducteur la mise en œuvre effective de certaines des obligations de vigilance à l'entrée en relation d'affaires.

3.5.2. Champ d'application

La tierce introduction ne peut porter que sur la mise en œuvre des obligations :

- d'identification et de vérification de l'identité du client et le cas échéant, du bénéficiaire effectif ;
- de recueil des éléments de connaissance de la relation d'affaires.

Lorsque les organismes financiers ont recours à un tiers pour la mise en œuvre d'autres mesures de vigilance (par exemple, l'obligation de vigilance constante), il s'agit alors d'externalisation. La tierce introduction se distingue également de l'externalisation en ce que les mesures de vigilance sont alors mises en œuvre par le tiers introducteur conformément à ses propres procédures LCB-FT.

3.5.3. Caractéristiques du tiers introducteur

Le tiers introducteur répond aux conditions de qualité et de localisation géographique suivantes :

- il est nécessairement soit un organisme financier (hors changeurs manuels, IOBSP et intermédiaires en financement participatif), soit un professionnel du chiffre et du droit ;
- il est établi, ou a son siège social, en France ou dans l'Union européenne ou l'Espace économique européen.

La sélection du tiers introducteur doit résulter d'une approche par les risques conduite par l'établissement assujetti. Cela consiste notamment à analyser formellement les risques potentiels encourus concernant le tiers introducteur (nature de l'activité du tiers, nature et objet de la relation d'affaires à envisager avec le client).

Les « cascades » de tiers introducteurs ne sont pas admises.

Une convention entre l'établissement assujetti et le tiers introducteur précise les modalités de la mise en œuvre des échanges d'informations. Cette convention n'exonère pas les parties de leurs obligations en matière de LCB-FT, l'établissement assujetti demeurant responsable de celles-ci.

Le dispositif de contrôle interne de l'établissement assujetti doit s'assurer du respect des dispositions propres à la tierce introduction.

Le tiers introducteur doit pouvoir mettre sans délai et à la première demande, à disposition de l'établissement assujetti, les informations nécessaires à la mise en œuvre des diligences de ce dernier.

4. L'OBLIGATION DE VIGILANCE

4.1. L'obligation de vigilance avant l'entrée en relation et tout au long de la relation

Tout établissement doit observer une vigilance constante : examen attentif des opérations par rapport à la connaissance actualisée du client, notamment lors de tout événement dans la relation client...

Les mesures de vigilance sont adaptées aux niveaux de risque présentés par le client et par l'opération : vigilance simplifiée, vigilance normale ou vigilance renforcée.

Il s'agit donc de mettre en place une « **approche par les risques** ».

Dans tous les cas, l'établissement doit prendre soin d'actualiser son dossier du client, ainsi que le profil risque LCB-FT de celui-ci tout au long de la relation d'affaires afin d'adopter la vigilance appropriée.

4.2. Les mesures de vigilance simplifiées

L'établissement peut mettre en œuvre des **mesures de vigilance simplifiées** dans les cas suivants :

- lorsque le **risque** de blanchiment des capitaux et de financement du terrorisme paraît **faible** à l'issue d'une analyse propre à cet établissement ;
- les **clients, les services ou les produits** présentent un **faible risque** de blanchiment de capitaux ou de financement du terrorisme par application de la réglementation, pour autant qu'il n'existe pas de soupçon de blanchiment.

En particulier la réglementation a déterminé que les **clients suivants pouvaient être considérés à risque faible** :

- un établissement financier ou une entreprise d'assurance de l'Union européenne ou de l'Espace économique européen ;
- une société cotée sur un marché réglementé de l'Union européenne ou de l'Espace économique européen ou un marché de pays tiers présentant des caractéristiques équivalentes⁵⁵ ;
- une autorité publique ou un organisme public de l'Union européenne ou de l'Espace économique européen qui satisfait à certains critères.

Pour pouvoir mettre en œuvre des mesures de vigilance simplifiées, l'établissement doit pouvoir justifier que son analyse aboutit à un risque faible ou fournir les documents prouvant que le produit ou le client appartient aux catégories mentionnées par la réglementation.

4.3. Les mesures de vigilance renforcées

L'établissement **doit** mettre en œuvre des **mesures de vigilance renforcées** dans les cas suivants :

- lorsque le **risque** de blanchiment des capitaux et de financement du terrorisme paraît **élevé** à l'issue d'une analyse propre à cet établissement ;
- lors **d'opérations favorisant l'anonymat** ;
- en cas de **relation d'affaires** avec des **personnes politiquement exposées** (PPE) (cf. ci-dessous au paragraphe 5, *Le cas particulier des personnes politiquement exposées*) ;
- lors **d'opérations effectuées** avec des personnes physiques ou des entités, y compris leurs filiales ou établissements, situées dans un pays où **la législation ou les pratiques en matière de LCB-FT sont jugées insuffisantes** ;
- en cas de relation de correspondant bancaire ou en vue de la distribution d'instruments financiers avec une société située hors de l'Union européenne ou de l'Espace économique européen ;
- en cas de **désignation par Tracfin d'opérations ou de personnes**.

Les renforcements des mesures de vigilance sont adaptés à chaque situation, notamment :

- demande d'une pièce d'identité supplémentaire ou certification de l'identité par une autorité ;
- recueil d'informations complémentaires sur la nature de la relation d'affaires, l'origine des fonds et du patrimoine du client et, le cas échéant, du bénéficiaire effectif ;
- décision d'entrée en relation avec une personne politiquement exposée prise par un membre de la direction de l'établissement assujéti ou une personne habilitée à cet effet ;
- alimentation initiale du compte par un transfert provenant d'un établissement financier de l'Union européenne ou de l'Espace économique européen ou d'un pays équivalent ;
- surveillance renforcée par l'augmentation du nombre et de la fréquence des contrôles réalisés et par l'adaptation des critères et seuils en fonction desquels les opérations doivent faire l'objet d'un examen plus approfondi ;
- limitation des relations d'affaires ou des transactions avec des personnes physiques ou tout autre entité provenant d'un État ou territoire à dispositif de LCB-FT insuffisant...

En outre, l'établissement **doit** mettre en œuvre des **mesures de vigilance renforcées**, matérialisées par un « examen renforcé », pour les opérations atypiques suivantes :

- **opérations particulièrement complexes** ;
- **opérations d'un montant inhabituellement élevé** ;
- **opérations ne paraissant pas avoir de justification économique ou d'objet licite**.

Lors de cet examen renforcé, l'établissement se renseigne auprès du client sur l'origine des fonds et la destination de ces sommes ainsi que sur l'objet de l'opération et l'identité de la personne qui en bénéficie.

⁵⁵ À cet effet, les établissements assujettis français déterminent la liste de ces pays tiers équivalents sur la base de sources crédibles. Ils ne peuvent plus se référer automatiquement à la liste fixée par l'arrêté du 27 juillet 2011.

5. CAS PARTICULIER DES « PERSONNES POLITIQUEMENT EXPOSÉES »

Entretenir des relations avec des personnes exerçant des fonctions politiques importantes expose l'établissement assujéti à des risques particuliers en matière de soutien financier du terrorisme, de tentative de corruption ou de circulation de capitaux d'origine frauduleuse à des fins de blanchiment.

Le dispositif de lutte contre le blanchiment impose des obligations particulières aux relations avec les **personnes politiquement exposées** (PPE et en anglais PEP).

L'obligation d'identification des personnes politiquement exposées vise non seulement les clients mais également les bénéficiaires effectifs des clients.

La décision d'entrée en relation avec une personne politiquement exposée doit être prise par un membre de la direction de l'établissement assujéti ou une personne habilitée à cet effet.

5.1. Définition générale

Une « personne politiquement exposée » (PPE) est une personne physique exposée à des risques particuliers en raison des fonctions politiques, juridictionnelles ou administratives qu'elle exerce ou a cessé d'exercer depuis moins d'un an.

La notion de personne politiquement exposée est élargie :

- aux **membres directs de sa famille** ;
- ou aux **personnes connues pour lui être étroitement associées**, telles que les personnes physiques qui sont bénéficiaires effectifs d'une personne morale détenue conjointement avec une personne politiquement exposée.



Zoom

Conditions de fonctions

Les fonctions des personnes politiquement exposées sont notamment les suivantes :

- chef d'État ou membre de gouvernement ;
- membre d'assemblée parlementaire ou dirigeant de parti politique ;
- ambassadeur, haut magistrat ou haut fonctionnaire ;
- dirigeant d'entreprise publique ou d'institution internationale.

5.2. Diligences complémentaires à la charge des établissements en relation avec une personne politiquement exposée

Les établissements doivent disposer d'une procédure spécifique pour détecter les clients ou bénéficiaires effectifs ayant la qualité de personne politiquement exposée, à l'entrée en relation d'affaires et tout au long de celle-ci.

Cette détection ne doit pas se fonder uniquement sur les déclarations des clients.

Une attention particulière est à porter dans les cas publics de corruption ou de criminalité organisée (par exemple, ceux dont les principaux médias nationaux ou internationaux se font l'écho), ou sur lesquels les autorités nationales ont communiqué (par exemple, appel à la vigilance de Tracfin à l'égard de certains pays, qui inclut les vigilances à l'égard des personnes politiquement exposées issues de ces pays).

Lorsque le client, ou son bénéficiaire effectif, est une personne politiquement exposée ou le devient au cours de la relation d'affaires, **l'établissement applique les mesures de vigilance complémentaires suivantes :**

- il s'assure que la décision de nouer ou maintenir une relation d'affaires avec cette personne politiquement exposée ne peut être prise que par un membre de la Direction générale ou une habilitée à cet effet ;
- il recherche, pour l'appréciation des risques de blanchiment de capitaux et de financement du terrorisme, l'origine du patrimoine et des fonds impliqués dans la relation d'affaires ou la transaction ;
- il renforce les mesures de vigilance.

Les mesures de vigilance ne sauraient conduire à entraver la réalisation, notamment par les personnes politiquement exposées qui résident ou qui exercent des activités professionnelles en France, des opérations financières normales de la clientèle, lorsqu'elles correspondent à leur profil et ne présentent pas de caractéristiques différentes de celles des autres clients dans des circonstances similaires.

Les exigences concernant les personnes politiquement exposées ont un caractère préventif et non pénal et ne devraient pas être interprétées comme les stigmatisant comme étant impliquées dans des activités criminelles.

L'identification des personnes politiquement exposées n'a donc pas pour objet de les exclure de la clientèle, ni de les soumettre à des questionnements sans lien avec l'objectif de maîtrise du risque de blanchiment.

6. L'OBLIGATION DE DÉTECTER LES OPÉRATIONS SUSPECTES

Dans le cadre de son obligation de vigilance constante lors de l'identification du client et lors de l'exécution des opérations pour son compte, l'établissement assujéti :

- doit réaliser un **examen attentif** des opérations au regard de la connaissance actualisée du client ;
- en présence de certaines opérations atypiques, effectuer un **examen renforcé** de ces opérations ;
- **en cas de doute**, effectuer une déclaration **de soupçon** auprès de Tracfin dans les plus brefs délais, sans en avertir le client.

6.1. La classification des risques

Les établissements assujettis doivent mettre en place une classification des risques (souvent dénommée cartographie des risques LCB-FT) leur permettant de mieux cerner les opérations pouvant contenir un risque LCB-FT.

Cette classification est spécifique à chaque établissement et est adaptée à ses activités.

Elle prend en compte les critères suivants :

- le **risque produit** :
 - nature des services ou produits offerts,
 - conditions de transaction proposées,
 - canaux de distribution utilisés ;
- le **risque client** : caractéristique du client ;
- le **risque pays** : pays de d'origine ou de destination des fonds.

Les tableaux ci-dessous illustrent des opérations pouvant générer des clignotants d'alerte.

6.2. Sur le marché des entreprises

Objet d'analyse	Indicateurs d'alerte éventuellement cumulatifs (et/ou)		
Client	Bénéficiaire effectif PPE	Activité à risque	Domiciliation dans un paradis fiscal
Sociétés écrans	Sociétés de domiciliation	Utilisation de prête-nom ou d'intermédiaire	Utilisation de comptes de passage
Espèces	Importance des dépôts et retraits	Récurrence non justifiée des opérations	Activité ne nécessitant pas l'usage d'espèces

Objet d'analyse	Indicateurs d'alerte éventuellement cumulatifs (et/ou)		
Fonctionnement du compte	Rapatriements suivis de transferts	Recours à l'urgence pour faire les opérations (pression du client)	Rotations rapides sans justification
Fonctionnement de compte inhabituel	Réactivation de comptes dormants	Forte progression du mouvement d'affaires d'un mois sur l'autre	Évolution exponentielle du chiffre d'affaires
Explications peu probantes du client	Anomalies dans les justificatifs transmis	Refus du client de fournir les justificatifs probants	Informations évoluant au cours de l'entrée en relation
Multiplication des opérations	Intra groupe	Entre comptes professionnels et comptes privés	Avec des sociétés situées dans des paradis fiscaux

6.3. Sur le marché des particuliers

Objet d'analyse	Indicateurs d'alerte éventuellement cumulatifs (et/ou)		
Espèces	Versements inhabituels au regard du patrimoine	Versements récurrents non justifiés	Suivis de transferts
Identité incertaine	Du donneur d'ordre	Du bénéficiaire	Des mandataires
Comptes de non-résidents	Informations difficiles à obtenir	Pays de résidence à risque	
Justification économique	Justification peu claire	Rendement systématiquement négatif	
Fonctionnement du compte	Réactivation de comptes dormants	Forte progression des encours d'un mois sur l'autre	
Mouvements financiers	Multiplis virements sur Internet	Nombreux mouvements financiers avec l'étranger	
Origine des fonds	Chèques représentatifs de gains de jeux	Remises déplacées dans plusieurs agences sans raison bien définie	
Connaissance actualisée du client	Décalage entre flux financiers et revenus	Décalage entre flux financiers et patrimoine	Décalage des flux financiers au regard de la situation professionnelle

6.4. Les diligences particulières dans le domaine de la gestion

■ Au passif



Zoom

Lors de la souscription de parts d'un fonds géré par une société de gestion de portefeuille, celle-ci doit considérer que le client est :

- la personne physique ou morale qui souscrit directement des parts du fonds pour son propre compte, et non pour le compte d'autres investisseurs sous-jacents ;
- l'établissement qui, dans le cadre de son activité de gestion, souscrit directement des parts en son nom pour le compte d'un tiers qui n'a pas pris la décision d'investissement ;
- l'intermédiaire financier, qui agit en son nom et qui est le propriétaire officiel des actions ou des parts, mais qui agit pour le compte et suivant les instructions spécifiques de tiers.

En matière de commercialisation d'organismes de placement collectif (OPC) :

- soit la société de gestion est en **contact direct avec l'investisseur** : elle est alors soumise aux mêmes règles d'identification, de contrôle et de déclaration que celles applicables à tous les prestataires de services d'investissement ;
- soit, comme cela est le plus fréquent, la **distribution s'effectue par l'intermédiaire d'un tiers** (le distributeur) et la société de gestion n'a pas connaissance du porteur final ou du bénéficiaire effectif, elle signe alors une **convention de distribution** avec ce tiers (une clause LCB-FT est généralement insérée dans cette convention).

L'obligation de vigilance de la société de gestion dépend du lieu du siège social du distributeur :

- si le distributeur est localisé dans l'Union européenne ou dans l'Espace économique européen ou dans un pays tiers équivalent, la société de gestion a **l'obligation de vérifier que le distributeur est bien agréé dans son pays d'origine**,
- sinon, la société de gestion a **l'obligation de vérifier l'identité du distributeur, de préciser, dans la convention de distribution, les diligences** que le distributeur devra réaliser (procédures équivalentes à celles qui sont appliquées dans l'Union européenne) et **d'obtenir du distributeur qu'il s'engage à mettre à disposition des éléments d'identification du client / du bénéficiaire effectif sur simple demande**.

Le dépositaire doit vérifier l'existence d'une telle convention.

■ À l'actif

Lors de la mise en œuvre de sa politique d'investissement pour compte propre ou pour compte de tiers, la société de gestion de portefeuille :

- veille à évaluer le risque de blanchiment de capitaux et de financement du terrorisme ;
- et définit des procédures permettant de contrôler les choix d'investissements opérés par ses collaborateurs.

Avant de procéder à des investissements, la société de gestion de portefeuille recueille les informations nécessaires lui permettant d'évaluer le risque de blanchiment de capitaux et de financement du terrorisme.

Les sociétés de gestion de portefeuille identifient les risques auxquels s'exposent leurs investissements de la même manière que les risques auxquels ils s'exposent dans la gestion de leur passif, en suivant les facteurs de risques évoqués plus haut, avec les particularités suivantes :

- **au titre du risque produits** : les sociétés de gestion de portefeuille **tiennent compte également des conditions de transaction proposées** (terme, co-investissement, importance de la participation envisagée, recours à des structures intermédiaires) **et des formes et modalités du sourcing** (recours à des apporteurs d'affaires) ;
- **au titre du risque pays** : les sociétés de gestion de portefeuille portent leur attention sur **la localisation des cibles** (si les sociétés ou les actifs immobiliers sont situés dans des pays à haut risque), **l'origine ou la destination des flux financiers** qu'impliquent les opérations d'investissement ;
- **au titre du risque clients ou, ici de contreparties** : les sociétés de gestion de portefeuille **prennent en compte la qualité de leurs cocontractants**, (personnes physiques ou morales), leur réputation, la présence de personnes politiquement exposées.

7. LE RÔLE DE TRACFIN

7.1. Les missions de Tracfin

Intervenant majeur dans la lutte contre le blanchiment de capitaux et le financement du terrorisme, **Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins)** est un service à compétence nationale rattaché au ministère de l'action et des comptes publics.

Tracfin est un **service d'enquête administrative** en charge de l'analyse des déclarations de soupçon adressées par les établissements assujettis à la réglementation LCB-FT.

Tracfin recueille, analyse, enrichit les déclarations de soupçon reçues. Il peut effectuer des contrôles sur place, au sein des établissements, à l'occasion d'opérations suspectes.

Il anime et coordonne les études et les actions nationales et internationales.

Il saisit le procureur de la République lorsqu'il identifie des faits susceptibles de relever du blanchiment de capitaux ou du financement du terrorisme.

Il désigne également, à l'attention des professionnels assujettis, des personnes ou des opérations qui présentent des risques élevés.

7.2. Les pouvoirs de Tracfin

■ Droit de communication

Tracfin a le droit de demander à un établissement financier de transmettre dans un certain délai des documents, quel qu'en soit le support, en relation avec le contenu de la déclaration.

■ Droit de consultation

Tracfin peut obtenir directement des pièces en se rendant dans les locaux des établissements financiers soumis au dispositif LCB-FT.

■ Droit d'opposition

Tracfin peut s'opposer ou suspendre l'exécution d'une opération pendant dix jours ouvrables à compter du jour d'émission de sa notification.

Il peut demander au président du Tribunal de grande instance de proroger ce délai après avis du procureur de la République.

7.3. La déclaration de soupçon auprès de Tracfin

■ Principes

Les professionnels assujettis à la réglementation LCB-FT sont tenus de déclarer à Tracfin :

- les soupçons sur les relations d'affaires ou les opérations ;
- les informations relatives à certaines catégories d'opérations.

Les opérations faisant l'objet d'une **déclaration** de soupçon à Tracfin : les sommes inscrites dans les livres ou les opérations portant sur des sommes dont les établissements :

- savent ;
- soupçonnent ;
- ont de bonnes raisons de soupçonner ;

qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à 1 an ou participent au financement du terrorisme.

La fraude fiscale n'est prise en considération qu'en présence d'au moins l'un des seize critères définis par décret.

■ Processus de déclaration

Les déclarations de soupçon sont effectuées après détection par l'établissement et analyse par la personne en charge d'effectuer ces déclarations au sein de l'établissement (le déclarant Tracfin).

Les déclarations peuvent aussi avoir lieu dans les contextes suivants :

- à l'issue d'un examen renforcé ;
- en complément d'une déclaration précédente ;
- pour infirmer, conforter ou modifier les informations fournies précédemment ;
- lors d'une tentative d'opération.

La déclaration s'effectue par Internet, par accès sécurisé ou sur support formalisé.

Les établissements financiers ont l'obligation d'adresser les déclarations via un système informatique mis en place par Tracfin (ERMES).

■ Moment de la déclaration

Les déclarations de soupçon sont adressées **sans délai** à Tracfin.

L'Établissement doit s'abstenir d'effectuer toute opération dont il soupçonne qu'elle est liée au blanchiment de capitaux ou au financement du terrorisme jusqu'à ce qu'il ait fait la déclaration de soupçon.

Lorsqu'une opération devant faire l'objet de la déclaration de soupçon a déjà été réalisée :

- soit parce qu'il a été impossible de surseoir à son exécution ;
- soit que son report aurait pu faire obstacle à des investigations ;
- soit que le soupçon est apparu postérieurement à la réalisation de l'opération ;

le déclarant Tracfin en informe sans délai Tracfin.

■ Contenu de la déclaration

La déclaration comporte :

- des éléments d'identification de l'organisme déclarant, d'identification et de connaissance des clients ;
- le descriptif précis et motivé des opérations suspectes concernées et les éléments d'analyse qui ont conduit le professionnel à l'effectuer.

■ Suivi de la déclaration

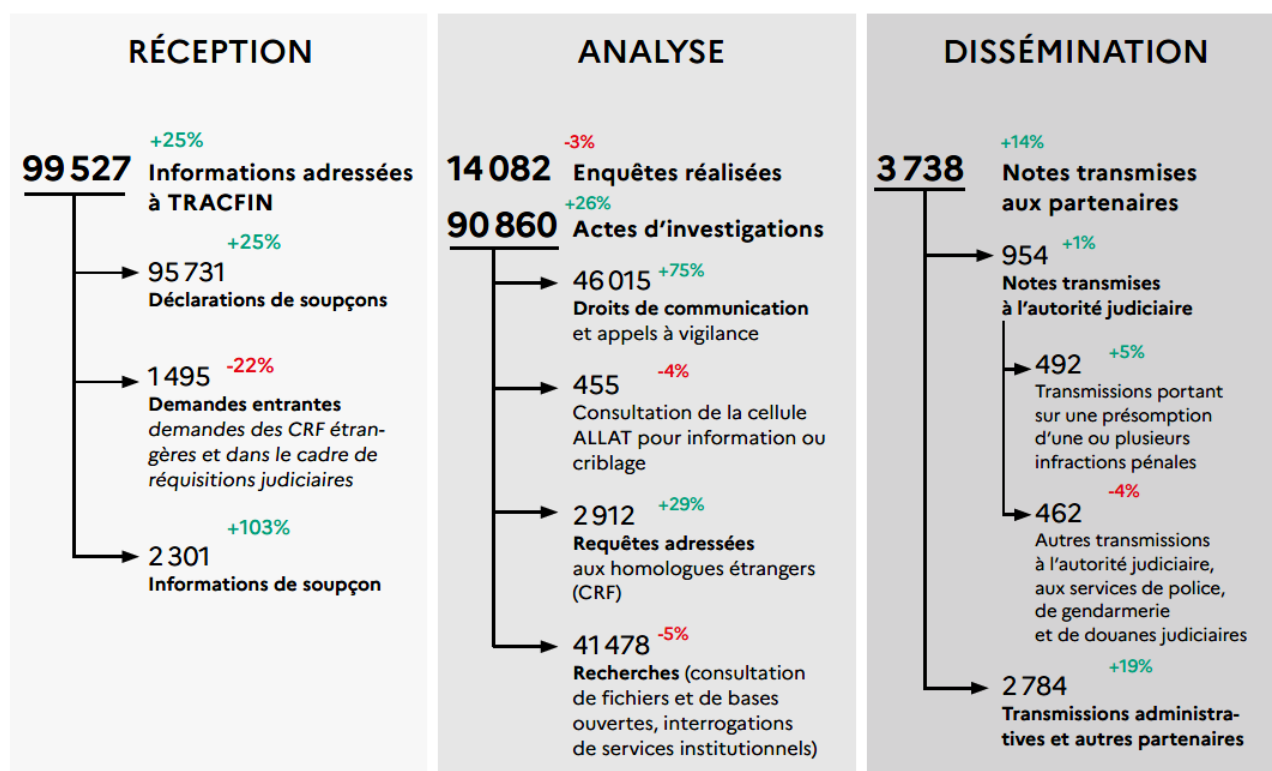
Tracfin accuse réception de la demande.

Il peut poursuivre ses investigations, y compris en effectuant des contrôles sur place.

Il peut exercer son droit d'opposition (cf. *supra*).

Il saisit, s'il y a lieu, le procureur de la République sans mentionner le nom de l'Établissement à l'origine du soupçon.

L'activité de Tracfin en 2019



Les pourcentages indiquent les évolutions au regard de 2018

Source : Rapport annuel 2019 de Tracfin

7.4. L'obligation de confidentialité

La déclaration de soupçon est confidentielle.

Il est interdit, sous peine de sanctions :

- **de porter à la connaissance du propriétaire des sommes ou de l'auteur de l'une des opérations (objets d'une déclaration de soupçon) ou à des tiers, autres que les autorités de contrôle, l'existence et le contenu d'une déclaration faite à Tracfin ;**
- **de donner des informations sur les suites qui ont été réservées à celle-ci.**

Tracfin ne peut communiquer la déclaration de soupçon transmise par un professionnel que sur réquisition émise par l'autorité judiciaire.

Les entreprises appartenant à un même groupe peuvent s'échanger des informations sous certaines conditions.

Certaines entreprises assujetties peuvent, lorsqu'elles interviennent pour un même client et dans une même opération, s'informer mutuellement de l'existence et du contenu de la déclaration de soupçon sous certaines conditions.

7.5. Les communications systématiques d'informations (COSI) à Tracfin

Certains établissements ont l'obligation d'adresser de manière systématique à Tracfin des informations relatives à des **opérations identifiées comme présentant un risque élevé de blanchiment ou de financement du terrorisme en raison du pays ou du territoire d'origine ou de destination des fonds, de la nature des opérations en cause ou des structures juridiques impliquées dans ces opérations** (« COSI »).

Les communications systématiques d'informations portent sur :

- **les opérations de transmission de fonds effectuées à partir d'un versement d'espèces ou au moyen de monnaie électronique, de montant minimum de 1 000 € par opération ou de 2 000 € cumulés par client sur un mois civil ;**
- **les dépôts ou retraits en espèces, supérieurs à 10 000 €, effectués sur un compte de dépôt ou de paiement ouvert au nom d'un client, autre qu'un organisme financier.**

Alors que les déclarations de soupçon portent sur des opérations suspectes, les communications systématiques d'informations sont définies par des critères objectifs. Néanmoins, la transmission d'une communication systématique d'informations ne dispense pas l'organisme financier d'effectuer, le cas échéant, une déclaration de soupçon sur le fondement du même flux financier.

8. LES IMPLICATIONS D'ORGANISATION DANS LES ÉTABLISSEMENTS FINANCIERS

Pour répondre à leurs obligations, les établissements financiers sont tenus de mettre en place une procédure et une organisation interne spécifiques à la lutte contre le blanchiment de capitaux et le financement du terrorisme, qui s'inscrivent dans leur dispositif de contrôle permanent.

Lorsqu'ils appartiennent à un groupe, et que l'entreprise mère a son siège social en France, ils mettent en œuvre un dispositif existant au niveau du groupe ainsi qu'une politique adaptée.

8.1. En termes de structure

Un membre de la direction générale de l'établissement doit être désigné comme responsable de la mise en œuvre du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Il peut déléguer tout ou partie de cette fonction à un tiers sous réserve que ce tiers dispose de l'autorité, des ressources et de l'expertise nécessaires et qu'il ne soit pas impliqué dans l'exécution des services et activités qu'il contrôle. Le délégant demeure toutefois responsable.

Les établissements nomment également :

- **Un « correspondant Tracfin »**

Il centralise les relations avec Tracfin et assure la diffusion au personnel des informations qui en émanent.

Il participe chaque année à la rédaction du rapport annuel et du questionnaire réglementaires relatifs à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

- **Un « déclarant Tracfin »**

Il recueille les alertes d'opérations suspectes détectées au sein de l'établissement et procède à leur analyse.

Il décide, en toute indépendance, d'effectuer une déclaration de soupçon auprès de Tracfin après analyse.

Il peut s'agir d'une seule et même personne.

Leurs noms sont communiqués à Tracfin et, suivant le cas, à l'ACPR ou à l'AMF.

8.2. En termes de fonctionnement

Chaque établissement financier :

- élabore, diffuse et actualise des procédures définissant les mesures et les diligences à mettre en œuvre au sein de l'établissement ;
- élabore une classification des risques identifiant les risques de LCB-FT auxquels l'établissement est exposé et adapte en conséquence les niveaux de vigilance ;
- met en place un système d'évaluation et de gestion des risques de blanchiment de capitaux et de financement du terrorisme ;
- organise des formations régulières et adaptées au profit des collaborateurs ;
- détecte les opérations suspectes, avec notamment l'utilisation d'outils informatisés ;
- met en œuvre un processus de traitement des alertes.

Les établissements financiers faisant partie d'un groupe coordonnent ces mesures avec les dispositifs propres au groupe.

Par ailleurs, pour répondre aux obligations liées au régime des sanctions économiques et financières (cf. paragraphe 10 *infra*), l'établissement doit disposer de procédures relatives aux embargos et au gel des avoirs.

8.3. En termes d'enregistrement et d'archivage

L'établissement enregistre systématiquement toute pièce justificative de l'identité du client.

Toute analyse du déclarant Tracfin doit faire l'objet d'une note formalisée, que cette analyse aboutisse ou non à une déclaration de soupçon.

L'établissement doit conserver les documents relatifs aux opérations pendant 5 ans et les documents relatifs aux dossiers d'identification du client pendant 5 ans après la cessation de la relation.

Les documents liés aux déclarations de soupçon doivent également être conservés 5 ans.

Les procédures de chaque établissement définissent :

- les documents à conserver en fonction du profil risque LCB-FT du client ;
- les conditions d'archivage de ces documents.

Ceux-ci doivent être tenus en permanence à la disposition de Tracfin et des autorités de tutelle.

8.4. En termes de contrôle

L'établissement doit procéder à :

- des contrôles réguliers du respect des procédures internes actualisées ;
- des contrôles du bon fonctionnement du dispositif avec *reporting* aux autorités de tutelle.

9. LES RISQUES DE SANCTION

9.1. Les sanctions pour les personnes physiques

- Sanctions pénales au titre du blanchiment simple : jusqu'à **5 ans d'emprisonnement et 375 000 € d'amende**.
- Sanctions pénales au titre du blanchiment aggravé : jusqu'à **10 ans d'emprisonnement et 750 000 € d'amende**.

Les peines d'amende peuvent être élevées jusqu'à la moitié de la valeur des biens ou des fonds sur lesquels ont porté les opérations de blanchiment.

Les personnes qui n'observent pas l'interdiction de divulgation de déclaration de soupçon (leur existence aussi bien que leur contenu) risquent d'être poursuivies pour complicité et être passibles d'une amende de 22 500 €.

9.2. Les sanctions pour les personnes morales

- Sanctions pénales au titre du blanchiment simple : jusqu'à 1 875 000 € d'amende.
- Sanctions pénales au titre du blanchiment aggravé : jusqu'à 3 750 000 € d'amende.

Les Commissions des sanctions de l'ACPR ou de l'AMF, selon la nature de l'établissement assujéti, appliquent par ailleurs des **sanctions disciplinaires** (avertissement, blâme, interdiction d'exercer ou retrait d'agrément, sanction pécuniaire).

■ Remarques

Ces sanctions sont lourdes de conséquences :

- pour le collaborateur éventuellement mis en cause ;
- pour l'organisme financier, en termes d'exercice de son activité et au regard du risque d'image et de réputation.

En revanche, les organismes, les dirigeants ou les employés qui **procèdent à une déclaration de bonne foi**, bénéficient **d'immunités** civiles, pénales ou professionnelles. Ces immunités s'appliquent même si la déclaration se révèle infondée dès lors qu'elle est effectuée de bonne foi. Les dirigeants et employés ne peuvent pas être poursuivis pénalement au titre de la violation du secret professionnel.

La responsabilité civile des organismes financiers ne peut pas être mise en cause par leurs clients. **C'est l'État qui répond du dommage éventuel.**

Lorsque l'opération financière a été **exécutée** après que l'organisme financier a effectué une déclaration conforme au service Tracfin non suivie d'opposition, l'organisme financier est dégagé de toute responsabilité. Sauf concertation frauduleuse, aucune poursuite pénale ne peut être engagée de ce fait contre ses dirigeants pour recel ou infraction de blanchiment d'argent.

10. LES RÉGIMES DE SANCTIONS ÉCONOMIQUES ET FINANCIÈRES

10.1. Présentation générale

Les régimes de sanctions économiques et financières poursuivent différents objectifs d'intérêt général, tels que la lutte contre le terrorisme, la lutte contre la prolifération des armes de destruction massive, la coercition en réaction à des violations graves des droits de l'homme ou à des actes menaçant la paix.

Les embargos et le gel des avoirs constituent les deux instruments principaux de ces sanctions.

10.2. Les embargos

Les **embargos** sont des **interdictions officielles portant sur les échanges commerciaux** avec un pays, un territoire, un gouvernement ou une juridiction.

Ils visent à **interdire le commerce de biens et de services ciblés** : pétrole, armes, matériels de prolifération, équipements et technologies clés dans les secteurs du pétrole et du gaz ou des télécommunications.

Ces mesures restrictives financières ou commerciales peuvent être décidées par l'ONU, le Conseil de l'Union européenne et la France vis-à-vis d'États, de zones géographiques, de secteurs d'activités ou de personnes morales.

10.3. Le gel des avoirs

Les mesures de gel des avoirs sont prises à l'égard de personnes, d'organismes et d'entités, visant notamment à **les empêcher de bénéficier ou de jouir de leurs fonds, de leurs ressources économiques, ainsi que de leurs transactions financières ou commerciales**.

Ces mesures de gel impliquent de geler sans délai les fonds et autres biens des personnes ou entités désignées par ces mesures, et de s'assurer qu'aucun fonds ou autre bien ne soit mis, directement ou indirectement, à la disposition ou utilisés au profit de ces personnes ou entités.

Il existe plusieurs régimes applicables en France aux personnes assujetties aux obligations de LCB-FT en matière de gel des avoirs :

- ceux issus des **résolutions du Conseil de sécurité des Nations Unies** qui doivent être transposées via des règlements européens d'application directe ;
- ceux consécutifs à des décisions de politique étrangère et de sécurité commune (PESC) du Conseil de l'Union européenne et mises en œuvre via l'adoption de règlements européens d'application directe, dans le cadre de la lutte contre le financement du terrorisme ou de sanctions à l'encontre de certains pays ;
- celui issu du régime français de gel des avoirs dans le cadre de la lutte contre le financement du terrorisme institué par le Code monétaire et financier, qui s'applique uniquement aux personnes qui détiennent ou reçoivent des fonds ou des ressources économiques pour le compte d'un client.



Zoom

Les fonds ou ressources économiques susceptibles d'être gelés recouvrent notamment :

- les fonds remboursables du public détenus ou versés sur des comptes de dépôts ou des comptes courants ou des comptes d'épargne tels que les livrets ;
- les fonds déposés ou détenus sur des comptes de paiement ;
- les fonds versés pour charger des instruments de monnaie électronique et les valeurs monétaires stockées sur ces instruments ;
- les fonds versés dans le cadre d'un contrat individuel ou collectif de gestion d'actifs ;
- les intérêts et autres revenus d'actifs financiers de toute nature (rémunération sur les comptes à vue, comptes d'épargne, parts d'OPCVM, actions de SICAV) ;
- les primes ou cotisations versées dans le cadre d'un contrat d'assurance et les indemnités versées ;
- les contrats d'assurance-vie ou de capitalisation.

10.4. La mise en œuvre des dispositifs au sein des établissements

Pour répondre aux obligations relatives aux embargos et au gel des avoirs, les établissements doivent procéder :

- à la **mise en place de filtres** pour détecter toute opération au bénéfice d'une personne ou d'une entité faisant l'objet d'une restriction au titre d'un embargo ;
- à la **tenue des listes des mesures de gel des avoirs** (européenne et nationale) et à la mise en place des **dispositifs d'application** en la matière.

Bien que non applicable directement sur le territoire français, les sanctions prises par les États-Unis et administrées par l'*Office of foreign assets contro*⁵⁶ (OFAC) peuvent avoir une portée extraterritoriale, même lorsque la transaction ne relève pas de la juridiction des États-Unis. Leur méconnaissance peut conduire les établissements financiers internationaux à de lourdes pénalités financières voire même à la perte de leur licence aux États-Unis.

11. L'ÉCHANGE AUTOMATIQUE ET OBLIGATOIRE DANS LE DOMAINE FISCAL

■ Présentation du dispositif

Afin de lutter contre la fraude et l'évasion fiscales, l'Union européenne a institué un régime d'échange automatique et obligatoire d'informations dans le domaine fiscal conforme à la norme commune de déclaration élaborée par l'Organisation de coopération et de développement économiques (OCDE).

Ce dispositif impose un échange obligatoire d'informations de nature fiscale entre administrations compétentes des États membres :

- de manière automatique, les informations suivantes :
 - revenus professionnels,
 - jetons de présence,
 - produits d'assurance sur la vie,
 - pensions,
 - propriété et revenus de biens immobiliers ;
- sur demande d'une autorité d'un État membre, les informations dont une autorité d'un autre État membre dispose ou que celle-ci obtient à la suite d'enquêtes administratives.

■ Son application en France

Les teneurs de compte, les organismes d'assurance et assimilés et toute autre institution financière déclarent à l'administration fiscale française les informations permettant un échange automatique d'informations fiscales relatives aux comptes financiers.

Il appartient à l'administration fiscale française de communiquer ces informations aux administrations compétentes des autres États membres relativement aux personnes résidant dans ces États.

12. LE DISPOSITIF FATCA (*FOREIGN ACCOUNT TAX COMPLIANCE ACT*)

■ Présentation du dispositif

Les États-Unis ont institué en 2010 un dispositif fiscal dénommé FATCA (*Foreign account tax compliance act*) dont l'objectif est **d'amener les établissements financiers non-américains** :

- à **identifier les clients résidents fiscaux américains** (*US persons*), personnes morales ou personnes physiques ;
- et à **permettre à l'administration fiscale américaine (IRS) de recevoir des informations de nature fiscale les concernant.**

⁵⁶ L'*Office of foreign assets control* (OFAC) dépend du Département du Trésor américain. Il gère l'application des sanctions économiques et commerciales décidées par les États-Unis.

Les informations sur les paiements effectués par les établissements financiers aux *US persons* doivent être transmises annuellement à l'administration fiscale américaine par les établissements financiers :

- soit directement à l'IRS ;
- soit par l'intermédiaire de leur propre administration fiscale en cas d'accord inter-gouvernemental.

Les **obligations des établissements financiers vis à vis de leur clientèle américaine** sont les suivantes :

- **identification des comptes**, nouveaux ou existants, détenus par une ou plusieurs *US persons* ;
- **obtention de l'accord du client pour la divulgation de ses informations** à l'administration fiscale américaine ;
- *reporting* annuel.

À défaut de coopération et de fourniture des informations exigées par l'administration américaine, une **retenue à la source de 30 % s'applique sur l'ensemble des flux de source américaine et sur les produits de cessions de titres américains du client contribuable américain**, voire, dans certains cas, de l'ensemble des clients de l'établissement financier lui-même.

■ Son application en France

Un accord inter-gouvernemental a été signé entre la France et les États-Unis en novembre 2013 et une loi française de septembre 2014 en autorise l'approbation. Cet accord précise les renseignements qui doivent être obtenus et échangés à partir de 2014.

Les établissements financiers font compléter, au moment de l'entrée en relation, une auto-certification fiscale à leurs clients afin de détecter les *US persons*.

13. LA LUTTE CONTRE LA CORRUPTION

13.1. L'acte de corruption

Constitue un acte de corruption le fait, pour une personne investie d'une fonction déterminée, publique ou privée :

- de **solliciter ou d'agréer, de proposer sans droit**, directement ou indirectement, **des offres, des promesses, des dons, des présents ou des avantages** quelconques ;
- pour qu'elle **accomplisse** ou qu'elle **s'abstienne d'accomplir un acte de sa fonction**, de sa mission ou de son mandat.

La corruption est dite **active** lorsque l'acte de corruption est à l'initiative de la personne qui corrompt et **passive** lorsque cet acte est à l'initiative de la personne qui est corrompue.

Ces délits sont réprimés par le Code pénal par des peines pouvant aller jusqu'à 10 ans d'emprisonnement et d'une amende d'un million d'euros, dont le montant peut être porté au double du produit tiré de l'infraction.

13.2. Le cadre juridique et réglementaire

Plusieurs textes internationaux se sont attachés à renforcer la lutte contre la corruption :

- la Convention de l'OCDE ;
- la Convention pénale du Conseil de l'Europe ;
- la Convention des Nations Unies contre la corruption.

En France, 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 II » a renforcé les obligations légales des entreprises.

Les présidents, les directeurs généraux et les gérants d'une société employant au moins 500 salariés, ou appartenant à un groupe de sociétés dont la société mère a son siège social en France et dont le chiffre d'affaires ou le chiffre d'affaires consolidé est supérieur à 100 millions d'euros, **sont tenus de prendre les mesures destinées à prévenir et à détecter la commission, en France ou à l'étranger, de faits de corruption ou de trafic d'influence.**

13.3. Les mesures et programme de conformité anticorruption

Les obligations du programme anticorruption reposent sur les mesures et procédures suivantes :

- un **code de conduite anticorruption intégré au règlement intérieur de l'entreprise** définissant et illustrant les différents types de comportements à proscrire comme étant susceptibles de caractériser des faits de corruption ou de trafic d'influence ;
- un **dispositif d'alerte interne** destiné à permettre le recueil des signalements émanant d'employés ;
- une **cartographie des risques** ; elle prend la forme d'une documentation régulièrement actualisée et destinée à identifier, analyser et hiérarchiser les risques d'exposition de la société à des sollicitations externes aux fins de corruption, en fonction notamment des secteurs d'activités et des zones géographiques dans lesquels la société exerce son activité ;
- des procédures d'évaluation de la situation des clients, fournisseurs de premier rang et intermédiaires au regard de la cartographie des risques ;
- des **procédures de contrôles comptables** destinées à s'assurer que les livres, registres et comptes ne sont pas utilisés pour masquer des faits de corruption ou de trafic d'influence ;
- un dispositif de formation destiné aux cadres et aux personnels les plus exposés aux risques de corruption et de trafic d'influence ;
- un **régime disciplinaire permettant de sanctionner les salariés** en cas de violation du code de conduite de la société ;
- un dispositif de contrôle et d'évaluation interne des mesures mises en œuvre.

13.4. L'Agence française anticorruption (AFA)

Placée auprès du ministre de la Justice et du ministre en charge du Budget, **l'Agence française anticorruption (AFA)** est un service à compétence nationale créé par la loi Sapin II.

■ Son champ d'intervention

- la corruption⁵⁷ ;
- le trafic d'influence ;
- le détournement de fonds publics ;
- le favoritisme ;
- la prise illégale d'intérêts ;
- la concussion.

■ Ses missions

L'Agence française anticorruption exerce **des missions de conseil et d'assistance**. À ce titre, elle assure la diffusion des informations et des bonnes pratiques permettant d'aider à prévenir et à détecter les atteintes à la probité.

Elle dispose également d'un pouvoir administratif de contrôle lui permettant de vérifier la réalité et l'efficacité des mécanismes de conformité anticorruption mis en œuvre, notamment par les entreprises (privées ou publiques), les administrations de l'État ou les collectivités territoriales.

Elle assure aussi le contrôle et le suivi de l'exécution des mesures judiciaires.

En cas de manquement constaté, le directeur de l'AFA communique le rapport de contrôle à la personne et la met en demeure de présenter ses observations écrites dans un délai de deux mois. À l'expiration de ce délai, il peut décider :

- de délivrer un avertissement ;
- de saisir la Commission des sanctions de l'Agence française anticorruption.

■ La Commission des sanctions de l'Agence française anticorruption

La Commission des sanctions peut :

- **enjoindre aux entreprises d'adapter les procédures de conformité** internes, selon les recommandations qu'elle leur adresse ;
- **prononcer une sanction pécuniaire** d'un montant pouvant aller jusqu'à 200 000 euros pour les personnes physiques et jusqu'à 1 million d'euros pour les personnes morales.

⁵⁷ Voir la définition des mots de cette liste dans le glossaire.

Pour aller plus loin

■ Sites Internet

- acpr.banque-france.fr
- amf-france.org/fr/reglementation/reglementation-accueil
- heconomie.gouv.fr/tracfin
- fatf-gafi.org/fr
- tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques
- agence-francaise-anticorruption.gouv.fr

■ Directive (UE) 2018/1673 du Parlement européen et du Conseil visant à lutter contre le blanchiment de capitaux au moyen du droit pénal, du 23 octobre 2018

■ Règlement UE n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS), du 23 juillet 2014

■ EBA / ESMA / EIOPA / *Joint committee of the European supervisory authorities* : (<https://esas-joint-committee.europa.eu/Publications/Guidelines>)

- Orientations communes, sur les mesures de vigilance simplifiées et renforcées à l'égard de la clientèle et sur les facteurs que les établissements de crédit et les établissements financiers devraient prendre en considération lorsqu'ils évaluent les risques de blanchiment de capitaux et de financement du terrorisme associés aux relations d'affaires individuelles et aux transactions conclues à titre occasionnel - Orientations sur les facteurs de risque
- Orientations communes concernant les caractéristiques d'une approche fondée sur les risques pour la surveillance en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et la marche à suivre dans le cadre de la surveillance fondée sur les risques - Orientations relatives à la surveillance fondée sur les risques
- Orientations communes, relatives aux mesures que les prestataires de services de paiement doivent prendre pour détecter des informations manquantes ou incomplètes sur le donneur d'ordre ou le bénéficiaire, ainsi que les procédures devant être mises en place pour gérer un transfert de fonds qui n'est pas accompagné des informations requises

■ Décrets

- Décret n° 2009-874 du 16 juillet 2009 pris pour l'application de l'article L.561-15-II du Code monétaire et financier
- Décret n° 2020-118 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme
- Décret n° 2020-119 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme

■ Code pénal

- Article 222-38
- Articles 324-1 à 324-9
- Article 421-2-2
- Articles 432-11, 433-1 à 433-2-1, 445-1 et 445-2

■ Code monétaire et financier

- Partie législative : articles L.561-1 à L.564-2
- Partie réglementaire : articles R.561-1 à R.563-5

■ Doctrine de l'Autorité de contrôle prudentiel et de résolution (ACPR)

- Lignes directrices relatives à l'identification, la vérification de l'identité et la connaissance de la clientèle
- Lignes directrices conjointes de l'ACPR et de Tracfin sur les obligations de déclaration et d'information à Tracfin
- Lignes directrices relatives aux personnes politiquement exposées (PPE)
- Lignes directrices conjointes de la Direction générale du Trésor et de l'ACPR sur la mise en œuvre des mesures de gel des avoirs
- Lignes directrices dans le domaine de la gestion de fortune
- Lignes directrices relatives au pilotage consolidé du dispositif de LCB-FT des groupes

■ AMF

- Règlement général de l'AMF
 - Articles 320-14 à 320-23 (gestion de FIA)
 - Articles 321-141 à 321-150 (gestion d'OPCVM)
- Doctrine de l'Autorité des marchés financiers (AMF)
 - Analyse sectorielle des risques de blanchiment de capitaux et de financement du terrorisme
 - Position AMF - DOC-2019-14 – Orientations sur les facteurs de risque
 - Position - recommandation AMF - DOC-2019-15 – Lignes directrices sur l'approche par les risques en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme
 - Position - recommandation AMF - DOC-2019-16 – Lignes directrices sur les obligations de vigilance à l'égard des clients et de leurs bénéficiaires effectifs
 - Position AMF - DOC-2019-17 – Lignes directrices sur la notion de personne politiquement exposée
 - Position - recommandation AMF - DOC-2019-18 – Lignes directrices sur l'obligation de déclaration à Tracfin
 - Guide AMF sur le gel des avoirs, juillet 2020

■ Publications

- GAFI / FATF
 - Les 40 Recommandations du GAFI
<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>
- Tracfin
 - Rapport du Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme (COLB)
(https://www.economie.gouv.fr/files/files/directions_services/tracfin/analyse-nationale-des-risques-lcb-ft-en-France-septembre-2019.pdf)
 - Guide d'information sur la lutte contre le blanchiment de capitaux et le financement du terrorisme
(https://www.economie.gouv.fr/files/guide_blanchiment.pdf)
 - Rapport annuel
(<https://www.economie.gouv.fr/tracfin/rapports-dactivite-et-danalyse>)
 - Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme
(<https://www.economie.gouv.fr/tracfin/rapport-tendances-et-analyse-des-risques-bcft-2018-2019>)