TRIBUNE

MARS 2021

AMLD6

Vers un élargissement des infractions de blanchiment ?

CGI BUSINESS CONSULTING

LA 6e DIRECTIVE CONTRE LE BLANCHIMENT DE CAPITAUX

La 6e directive de l'Union Européenne contre le blanchiment d'argent et le financement du terrorisme est entrée en vigueur le 3 décembre 2020 et doit être mise en œuvre par les institutions financières d'ici le 3 juin 2021.

Après la 4e et la 5e directive, qui ont renforcé les dispositions existantes en matière de LCB/FT, la 6e directive vise à harmoniser le cadre européen et à soumettre le blanchiment de capitaux dans tous les États membres à des sanctions pénales effectives, proportionnées et dissuasives.
Les entités assujetties et autres parties prenantes doivent s'attendre à un contrôle accru de leurs programmes de gestion des risques et de conformité en matière de LCB/FT par les régulateurs nécessitant de mettre en place des actions de revue et de mise à jour des politiques, procédures, processus et des outils de détection des transactions atypiques.

Une définition plus complète de l'activité criminelle

La 6e directive LCB/FT dresse une liste de **22 infractions de blanchiment** de capitaux que tous les États membres de l'UE ont érigé en infraction pénale dans leur législation nationale :

- **Corruption**
- **Fraude**
- Participation à un groupe criminel organisé et racket d'extorsion
- Terrorisme
- **Cybercriminalité**
- Piraterie
- Traite des êtres humains et trafic illicite de migrants
- Exploitation sexuelle
- Trafic illicite de stupéfiants et de substances psychotropes
- Trafic d'armes
- Trafic illicite de biens volés et d'autres biens
- Contrefaçon de monnaie
- Contrefaçon et piratage de produits
- **Infractions contre l'environnement**
- Meurtre et blessures corporelles graves
- Enlèvement, séquestration et prise d'otage
- Vol avec ou sans violences
- Contrebande
- Infractions fiscales liées aux impôts directs et indirects
- Extorsion
- Faux
- Délit d'initié et manipulation de marché

L'introduction de nouvelles infractions dans le champ du blanchiment de capitaux et du financement du terrorisme nécessite que les institutions financières **réévaluent leurs mécanismes, leurs processus, leur appétit au risque et s'assurent que leurs programmes de conformité restent pertinents et adéquates.**

De plus, la 6e directive ne vise plus uniquement ceux qui profitaient directement de l'acte de blanchiment, mais également les « facilitateurs ou complices » qui seront également coupables sur le plan juridique.

La responsabilité et les sanctions de personnes morales

La 6e directive étend la responsabilité pénale aux personnes morales ainsi qu'aux personnes physiques ayant un pouvoir de représentation de la personne morale ; ayant autorité pour prendre une décision au nom de la personne morale ou pour exercer un contrôle en son sein.

Concrètement, cela signifie qu'une personne morale sera considérée comme coupable du crime de blanchiment d'argent s'il est établi qu'elle n'a pas empêché un « esprit dirigeant » de l'entreprise de mener l'activité illégale.

Une meilleure coopération internationale

Les dispositions de la 6e directive exigent des États membres de l'UE qu'ils criminalisent certaines infractions principales, qu'elles soient illégales ou non dans cette juridiction. Ces infractions principales sont le terrorisme, le trafic de drogue, la traite des êtres humains, l'exploitation sexuelle, le racket et la corruption.

Dans ce cadre, les États membres travailleront ensemble pour centraliser les procédures judiciaires au sein d'une seule juridiction. Les autorités prendront en compte certains facteurs de risque tels que le pays d'origine de la victime, la nationalité (ou la résidence) de l'auteur de l'infraction et la juridiction dans laquelle l'infraction a eu lieu pour décider de la façon de mener les poursuites.

Des mesures punitives renforcées

Les mesures punitives ont été renforcées pour les particuliers et certaines ont été introduites pour les personnes morales. La peine minimale d'emprisonnement pour les infractions de blanchiment d'argent sera de 4 ans.

Les mesures punitives applicables aux organisations/personnes morales comprennent la confiscation des activités commerciales, l'exclusion de l'accès au financement public ou même la liquidation judiciaire. Les entreprises devront envisager de renforcer leurs efforts de lutte contre le blanchiment d'argent et le financement du terrorisme afin de réduire le risque de poursuites pénales.

Les nouvelles infractions et les dispositifs LCB/FT

L'évolution réglementaire majeure de la 6e directive est l'élargissement des infractions de blanchiment de capitaux à d'autres infractions telles **que la fraude et la corruption, la cybercriminalité, les crimes environnementaux** incitant les institutions financières à opérer une transformation de leur organisation de la sécurité financière à la criminalité financière.

Dès 2019, TracFin met d'ailleurs l'accent sur la criminalité organisée, les manquements au devoir de probité ou corruption au sens large, la fraude fiscale et sociale, la cybercriminalité dans un rapport consacré aux tendances en matière de blanchiment de capitaux et de financement du terrorisme.

Les infractions de fraude et de corruption

Les pratiques de corruption peuvent prendre de nombreuses formes comme le versement de pots-de-vin, le paiement de facilitation, la falsification de données de facturation, l'extorsion, le favoritisme, le népotisme, la collusion, le détournement de fonds, la malversation, le trafic d'influence. La corruption est généralement engagée dans le but d'obtenir des gains financiers nécessitant généralement de blanchir les fonds issus de la corruption par des mécanismes appropriés.

Les pratiques de fraude ont tendance à évoluer avec l'émergence et le développement des entrées en relation d'affaires à distance qui favorisent certains types de fraude comme l'usurpation d'identité et la fraude documentaire. En effet, la digitalisation des relations d'affaires facilite le recyclage de faux documents d'identité et l'exploitation de preuves d'identité frauduleusement usurpées (utilisation de documents d'identité volés conjuguée à l'usage d'un VPN ou du réseau TOR pour masquer l'adresse IP de l'utilisateur).

La 6e directive offre aux institutions financières et à toutes les entreprises également assujetties à la loi Sapin 2 des pistes de mutualisation et d'optimisation des coûts des dispositifs LCB/FT et de lutte contre la fraude et la corruption notamment la cartographie des risques, le dispositif d'évaluation des tiers et le dispositif de gestion des alertes.

Les infractions environnementales

La criminalité environnementale n'a pas de définition juridique précise. On considère qu'elle englobe les **activités illégales qui nuisent à l'environnement** comme l'émission de polluants affectant l'eau, l'air ou le sol, la mise en danger d'espèces menacées, la mise en danger d'autrui ou de l'environnement par une mauvaise gestion de déchets dangereux, toxiques ou radioactifs, l'exploitation ou surexploitation illégale d'une ressource ou le non-respect d'une législation environnementale ayant entrainé de graves conséquences pour l'environnement ou la santé.

Le blanchiment d'argent et les crimes environnementaux sont directement liés par le processus de blanchiment des produits d'activités illégales favorisées par la faiblesse de la réglementation de nombreux pays. Des entreprises légitimes pourront être utilisées comme couverture des activités illicites, soit par dissimulation de la véritable nature de l'entreprise derrière une société écran, soit par association à des activités licites.

La cybercriminalité

Les pratiques de cybercriminalité sont très évolutives et peuvent prendre diverses formes telles que le vol direct par piratage informatique de l'argent ou des données sensibles, le vol indirect, par « hameçonnage » (ou phishing), l'exploitation des vulnérabilités d'un système d'information via un « logiciel malveillant » (ou malware), ou l'utilisation du cyberespace Deep ou Dark pour conduire anonymement des activités criminelles ou blanchir les bénéfices d'escroqueries.

Les conséquences de ces pratiques vont de **l'extorsion de fonds** par virements frauduleux à **l'usurpation d'identité.** Bien entendu, le contexte général de digitalisation des services de paiement et des relations d'affaires favorise une exposition importante aux fraudes et usurpations d'identité, notamment dans les secteurs des cryptoactifs, du financement participatif et de la banque en ligne. Le blanchiment des capitaux issus des activités cybercriminelles nécessite parfois la mise en place de circuits complexes avec notamment l'usage de mules (money mules) permettant l'exfiltration et la dissimulation des fonds volés par placements sur des comptes bancaires.

De la Sécurité Financière à la délinquance financière

L'élargissement des infractions entrant dans le champ du blanchiment de capitaux amène les institutions financières à revoir leur **organisation** et leurs **dispositifs LCB/FT** en ajustant notamment les **processus et les outils** de connaissance des clients (KYC), de détection et de surveillance des opérations atypiques et de gestion des alertes. Les collaborateurs à profils analystes ou investigateurs devront également être formés de façon prioritaire à la détection des nouvelles infractions de blanchiment.

Ainsi, c'est l'ensemble du pilotage opérationnel de la Sécurité Financière qui évolue vers un modèle plus large de lutte contre la **Criminalité Financière.**

La notion de criminalité financière s'étend alors à des sujets traités hors du scope de la conformité tels que les crimes environnementaux ou la cybercriminalité. Cette transformation favorise ainsi une **approche transversale de la réglementation** (6e directive, Loi Sapin 2, Loi sur le Devoir de Vigilance, Déclaration de Performance Extra-Financière, Plan d'action de l'UE sur la Finance Durable et règlements associés).

L'entrée en relation d'affaires digitalisée

Les mutations technologiques et la multiplication des pratiques criminelles associées à la fluidification des expériences clients via des solutions digitales, poussent les institutions financières à exercer une vigilance accrue de l'entrée en relation à distance et de la gestion documentaire.

En effet, la digitalisation des processus d'**entrée en relation d'affaires** (délais plus courts, relation à distance, authentification renforcée…), et l'optimisation de la **gestion documentaire** (de la collecte à l'archivage) simplifie d'une part l'expérience client et d'autre part fiabilise la connaissance client.

Ainsi l'identification digitale apparait comme un levier de performance et de fiabilisation : respect des mesures LCB/FT, optimisation du temps nécessaire à l'échange des documents, réduction des coûts ou amélioration de la confiance sur l'origine des documents.

Par ailleurs, l'offre FinTech de KYC digitalisé pose les pistes d'évolution de ces dispositifs avec le contrôle de documents automatisés, l'authentification du client par reconnaissance biométrique, le partage des données KYC grâce à la blockchain.

Surveillance, filtrage et gestion des alertes

Globalement ce sont les dispositifs de surveillance, de filtrage et de gestion des alertes qui sont impactés par les évolutions de la 6e directive puisque les systèmes doivent être adaptés à la détection des nouvelles infractions par la génération d'alertes sur de nouveaux scénarios de transactions atypiques.

Les déclarations de soupçon transmises à TRACFIN évolueront également pour inclure entre autres des données plus structurées et des analyses spécifiques à ces infractions.

En conclusion

La 6e directive et l'élargissement des infractions de blanchiment à 22 autres infractions autorisent désormais une lecture transversale de la réglementation ouvrant la Sécurité Financière à un terme plus générique de Criminalité ou Délinquance Financière.

Cette évolution constitue une opportunité de transformation et de mutualisation des ressources et des moyens mis en oeuvre dans la lutte contre le blanchiment des capitaux issus d'activités illicites telles que la fraude, la corruption, la cybercriminalité ou les crimes environnementaux.
Transformation et mutualisation prennent alors de multiples formes comme la mise en oeuvre d'une communication transverse des équipes, le partage et la centralisation des données, l'enrichissement des vérifications KYC (informations négatives élargies, Harwell Management nouvelles listes d'interdiction, nouvelles typologies de clients à risque), la gestion centralisée des alertes, le partage d'informations d'analyse et d'investigation, la mise en place de scénarios croisés de détection des opérations atypiques, la formation des collaborateurs et plus largement la gestion des incidents et des dispositifs de maîtrise des risques.

L’accompagnement Harwell Management

Harwell Management vous accompagne dans la mise en place et l’ajustement de vos dispositifs LCB/FT dans le cadre de l’intégration des évolutions de la 6e Directive contre le blanchiment, et plus largement dans la transformation et la mutualisation de l’ensemble des dispositifs de conformité ou de gestion et de maîtrise des risques de délinquance financière.

CGI BUSINESS CONSULTING

Chez CGI Business Consulting, cabinet de conseil majeur en France, nous sommes audacieux par nature. Grâce à son intimité sectorielle et à sa capacité à mobiliser des expertises diverses, CGI Business Consulting apporte aux entreprises et aux organisations des solutions de conseil audacieuses et sur mesure, pour une réussite stratégique et opérationnelle de leurs projets de transformation. Nos 1 000 consultants accompagnent nos clients dans la conduite et la mise en œuvre de leurs projets de transformation, dans une relation franche et de confiance, pour leur permettre de prendre les bonnes décisions. Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Elle aide ses clients à atteindre leurs objectifs, notamment à devenir des organisations numériques axées sur le client.

L'audace par nature