INFORMATIQUE RÉGLEMENTAIRE

Automatisation de la prévention contre le blanchiment dans les banques

Dans la lutte contre le blanchiment et le financement du terrorisme, les entreprises bancaires consacrent des moyens importants et mettent en œuvre des nouvelles technologies.

GEORGES CARDON
Chef de mission
lutte contre
le blanchiment
CNCE

Les entreprises bancaires ont depuis longtemps pris conscience de la nécessité de lutter contre le blanchiment et de se protéger contre les activités financières criminelles, tout en respectant leurs obligations professionnelles.

Force est de constater que la mobilisation visant à renforcer les dispositifs internationaux et nationaux de lutte contre ces menaces se traduit pour les banques et institutions financières par un accroissement continu des charges et des responsabilités qu'elles assument.

L'arsenal législatif et réglementaire français, au cours des dernières années, a considérablement étendu les obligations de surveillance et détection des opérations « douteuses » et a conduit les banques à se doter de véritables « cellules de veille », à repenser leur organisation interne, à mettre en place des procédures spécifiques, à former leur personnel, etc.

Les banques doivent faire preuve d'une vigilance constante, disposer d'un système de surveillance permanent et mettre en place des outils d'alerte efficaces permettant de déceler les opérations susceptibles de comporter un soupçon de blanchiment et la transmission de l'information à la cellule Tracfin, responsable, en France, du traitement du renseignement et de l'action contre les circuits financiers clandestins.

Pour autant, les risques inhérents à une défaillance dans le dispositif de prévention, pèsent sur les établissements et peuvent se traduire par des sanctions juridiques, financières et ainsi mettre en jeu leur réputation.

Une automatisation indispensable

En France et à l'étranger, l'actualité montre que ces risques ne sont pas virtuels, car les autorités de contrôle bancaire se montrent extrêmement sévères lorsqu'elles constatent des faiblesses dans la qualité des dispositifs de prévention mis en place. Ainsi, l'idée de recourir à des dispositifs automatisés pour améliorer l'efficacité de la surveillance se développe progressivement en France, alors que d'autres pays comme la Grande-Bretagne, les États-Unis et la Suisse sont en avance dans ce domaine.

Face à l'ampleur des risques, cette automatisation devient indispensable, notamment pour des banques de réseau multimétiers, disposant de vastes portefeuilles de clientèles, gérant d'importants volumes d'opérations, et mettant plusieurs canaux de distribution à la disposition de leurs clients.

L'automatisation repose, à partir du principe KYC (*Know your customer*) de connaissance du client, sur l'établissement de règles de gestion concernant la notion de profil client et de profil de fonctionnement des comptes, afin de pister les comportements inhabituels des clients ou de leurs comptes. Cette approche introduit une nouveauté dans le mode de gestion de la relation client

dans la banque et pose de multiples questions sur les moyens de détermination d'une « déviance » comportementale, à l'échelle de la variété des typologies de clientèles dans une banque à réseau. Ceci suppose la possibilité d'appréhender un profil défini à l'aide de critères objectifs, liés à l'activité, aux revenus, à la typologie des transactions, etc., et de pouvoir comparer les mouvements qui apparaîtraient en anomalie par rapport à ce profil.

De la même façon, l'historique et la nature des transactions pendant une période donnée doivent permettre de déceler des « anomalies », dès lors qu'on observe des modifications remarquables par rapport à cet historique.

Un projet qui comporte des impacts importants

À cette approche par profil, d'autres indicateurs liés à l'observation des formes de blanchiment peuvent être ajoutés, tels que les dépôts et retraits simultanés, la réactivation de comptes « dormants », les opérations générant une perte pour le client, etc.

La mise en place d'un système de surveillance automatisé est un projet qui comporte des impacts techniques, organisationnels et humains importants et qui suppose un appui déterminé de l'exécutif de la banque pour faire adhérer l'ensemble des acteurs concernés.

En effet, outre les inévitables problèmes de calibrage de l'outil (un calibrage « grossier » génère un nombre trop important de fausses alertes, et à l'inverse des seuils trop élevés risquent de laisser passer des cas de blanchiment), il convient de repenser les circuits de communication entre le système de production des alertes et leur analyse par le réseau commercial, et également le repositionnement des cellules de surveillance (correspondants Tracfin) jusqu'ici généralement rattachées à l'audit interne, qui se transforment en fonction opérationnelle.

Les banques peuvent donc envisager d'entreprendre un projet d'automatisation de la surveillance par développement interne. Cependant, de tels développements requièrent la mobilisation de moyens humains et technologiques importants. Le recours à des éditeurs, actuellement pour la plupart d'origine anglo-saxonne, permet de bénéficier de l'expertise acquise et d'allouer ainsi les ressources internes disponibles à d'autres chantiers.

Éviter l'effet « boîte noire »

Le choix d'une solution de marché implique d'étudier non seulement la compatibilité technique des outils avec les applicatifs existants et leur interfaçage, mais également la facilité d'alimentation de l'outil en données provenant des systèmes d'information, la facilité de paramétrage et aussi la qualité ergonomique de la solution.

Dans l'offre actuelle du marché, un des critères majeurs de choix est l'auditabilité de la solution, afin d'éviter l'effet de « boîte noire » et, par ailleurs, compte tenu de l'évolution constante du cadre réglementaire, il est préférable de privilégier une solution techniquement souple et adaptable.

Entreprendre un projet d'automatisation de la prévention du blanchiment implique de maîtriser son caractère transversal dans l'établissement et d'évaluer son impact sur le réseau commercial, ce qui nécessite un effort important de pédagogie et de soutien pour la prise en main d'une solution novatrice.

Conduite de projet « Automatisation de la prévention anti-blanchiment »

Le Groupe Caisse d'épargne, à la suite d'une large concertation interne associant les fonctions concernées du réseau et des filiales, a opté pour le déploiement de la solution Aristion + proposée par MasterCard/Alti pour la surveillance des opérations et le déclenchement d'alerte sur les cas douteux.

Ce projet qui mobilise actuellement un grand nombre d'acteurs issus des établissements du groupe et des communautés informatiques, est complété par une démarche spécifique d'accompagnement du changement pour la prise en main de l'outil, par le réseau commercial, à l'échéance de 2005 qui marquera l'aboutissement de la démarche entreprise par la CNCE pour doter le groupe d'un dispositif complet en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme. ¤