Forbes INSIGHTS

NE BLÂMONS PAS LES SYSTÈMES DE SURVEILLANCE DES TRANSACTIONS

COMMENT UNE APPROCHE RELATIONNELLE AMÉLIORE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET RÉDUIT LES COÛTS

EN COLLABORATION AVEC : pitney bowes

Table des matières

Introduction 2

Ne blâmons pas les TMS 4

Individus, processus et technologies : les trois piliers de la conformité 6

Au-delà des transactions 8

Une approche relationnelle 9

Exploiter au mieux les données « libres » 12

Révéler des liens grâce aux bases de données graphe 13

Obtenir une vision globale 14

Points clés et conseils 16

Conclusion 19

Remerciements 20

Introduction

Nul doute que la criminalité financière est un fléau grandissant. Sur le plan mondial, le blanchiment d'argent représenterait entre 1 000 et 2 000 milliards de dollars par an, soit entre 2 % et 5 % du PIB mondial.[1]

L'écrasante majorité de cet argent va à des organisations impliquées dans le trafic de drogues, d'armes et d'êtres humains, ou est utilisée pour financer des activités terroristes. Le département du Trésor des États-Unis, dans son rapport *National Money Laundering Risk Assessment*[2] de 2015, a décrit la lutte contre le blanchiment d'argent et le financement du terrorisme comme « un enjeu essentiel pour la sécurité nationale américaine et un système financier puissant ». Cependant, bien que près de 70 % de ces transactions illégales transitent par des institutions financières légitimes, l'Office des Nations Unies contre la drogue et le crime estime que moins de 1 % des capitaux blanchis est saisi et gelé.[3]

Compte tenu de cela, il n'est sans doute pas surprenant que les régulateurs financiers soient aujourd'hui plus stricts en ce qui concerne l'application des lois. Qu'il s'agisse de la connaissance client (KYC) ou de la loi sur le secret bancaire (Bank Secrecy Act, BSA) aux États-Unis, de la quatrième directive européenne anti-blanchiment ou des nombreuses mesures législatives d'autres pays, les banques sont soumises à des réglementations toujours plus strictes. Depuis la crise financière de 2008, les régulateurs, en particulier aux États-Unis, ont infligé des amendes record aux institutions financières pour avoir mené des transactions avec des parties ou des pays non autorisés, ou pour avoir manqué de se conformer aux initiatives de lutte contre le blanchiment d'argent.

Si les milliards de dollars d'amendes infligées à des institutions financières comme BNP Paribas font les gros titres, la plupart des accusations portent sur des violations de la réglementation (dans le cas de BNP Paribas, des transactions avec des pays non autorisés) qui vont au-delà de simples non-conformités et qui constituent des violations délibérées de la loi. Cependant, un simple tour d'horizon de l'actualité récente fait apparaître des pénalités de plusieurs millions de dollars infligées à des institutions qui ne semblent pas avoir volontairement bafoué la réglementation. Un récent communiqué de presse de la Financial Industry Regulatory Authority (FINRA) a rapporté[4] une amende de 17 millions de dollars contre une institution financière pour « ne pas avoir établi et mis en place des procédures adéquates de lutte contre le blanchiment d'argent, ce qui a empêché l'entreprise d'anticiper ou de détecter, d'enquêter et de signaler des activités suspectes pendant plusieurs années », ainsi qu'une amende de 25 000 dollars et une suspension de trois mois pour le responsable de la conformité anti-blanchiment d'argent de l'institution.

Les conséquences de ces pénalités vont au-delà de l'aspect financier. « S'il est vrai qu'un milliard de dollars représentent peu dans le bilan financier de banques comme HSBC ou Standard Chartered, la sanction peut coûter très cher en termes d'image », commente Julie Conroy, directrice de recherche chez Aite Group, une société de conseils en services financiers. « Le prix de leurs actions tend à être impacté ; et même s'il est difficile de quantifier la publicité négative, elle a de toute évidence des conséquences néfastes sur les entreprises. » En effet, comme le remarque Doug Stevenson, directeur général, Global Financial Crimes and Compliance chez Pitney Bowes : « personne ne veut être considéré comme la banque qui a financé le terrorisme ».

L'analyse publiée par le Center for Economic and Policy Research (CEPR),[5] un centre de recherche économique progressiste, rejoint les

1 *Estimating illicit financial flows resulting from drug trafficking and other transnational organised crimes.* (2011). Vienne. Extrait de https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
2 Département du Trésor des États-Unis. (2015). *National Money Laundering Risk Assessment.* Washington, D.C. : Département du Trésor. Extrait de https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf
3 *Estimating illicit financial flows resulting from drug trafficking and other transnational organised crimes.* (2011). Vienne. Extrait de https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
4 FINRA. (18 mai 2016). *FINRA Fines Raymond James $17 Million for Systemic Anti-Money Laundering Compliance Failures* [Communiqué de presse]. Extrait le 1er décembre 2016 de http://www.finra.org/newsroom/2016/finra-fines-raymond-james-17-million-systemic-anti-money-laundering-compliance
5 Armour J., Mayer C., & Polo A. (24 mars 2016). *Financial market wrongdoing: Fines vs reputational sanctions.* Extrait le 1er décembre 2016, de http://voxeu.org/article/financial-market-wrongdoing-fines-vs-reputational-sanctions

propos de Julie Conroy, en suggérant que les réactions du marché boursier à ces amendes peuvent représenter des coûts « en moyenne neuf fois supérieurs au montant des pénalités financières imposées par les régulateurs ».

Cette situation laisse les institutions financières en mauvaise posture, car elles doivent faire face aux coûts exorbitants liés aux différents aspects de la conformité et à des processus rapidement dépassés par les exigences des régulateurs. La conformité elle-même est un processus imparfait, souvent complexifiée par l'obsolescence des logiciels utilisés au sein des banques, ainsi que par les silos d'informations stockées dans les différents systèmes et secteurs d'activités. C'est pourquoi il s'avère aussi difficile de réellement connaître ses clients.

Les institutions financières s'adaptent en s'appuyant sur les systèmes de surveillance des transactions (Transaction Monitoring System, TMS) pour détecter les activités potentiellement suspectes et, en conséquence, les enquêteurs passent la majorité de leur temps à examiner de fausses alertes. Des observations suggèrent qu'entre 95 % et 98 % des alertes émises par ces systèmes sont des faux positifs, et comme chaque alerte nécessite traditionnellement entre cinq et quinze minutes de vérification (voire 45 minutes à plusieurs heures et jours pour les rapports d'activités suspectes), le gaspillage de ressources dans ces enquêtes est énorme.

Jim Burnick, directeur général, Financial Services Solutions chez Pitney Bowes, souligne que ce type de gaspillage ne serait pas toléré dans d'autres secteurs de l'entreprise. « On vous remplacerait vous et votre service, et votre budget serait réduit, car un rendement de 2 % dans un autre secteur serait catastrophique », explique-t-il. « Cependant, en matière de conformité, [les banques] sont prêtes à trier tous ces faux positifs afin d'être sûres de détecter les criminels qui font tout pour ne pas éveiller les soupçons. »

Heureusement, les avancées technologiques récentes permettent aux institutions financières de réduire les coûts de la conformité sans avoir à remplacer intégralement leurs systèmes de surveillance des transactions. En adoptant une approche relationnelle qui complète et soutient les TMS existants, les institutions peuvent atteindre un double objectif : réduire les faux positifs et accroître la conformité. Cette nouvelle approche associe les initiatives de qualité des données et la résolution d'entité à une base de données graphe pour favoriser la conformité de trois manières : en localisant les données sur les parties concernées quel que soit l'emplacement de ces données au sein de l'institution, en associant les parties et les transactions correspondantes, même lorsque les liens ne sont pas évidents et/ou sont délibérément camouflés, et en visualisant les relations de façon à pouvoir identifier rapidement et facilement les anomalies.

En s'appuyant sur des entretiens avec des experts et analystes du secteur financier et des professionnels des technologies, ce rapport examine comment une approche relationnelle et globale peut aider les institutions à réduire les coûts et les risques tout en améliorant considérablement le flux de travail et l'efficacité.

NE BLÂMONS PAS LES TMS

Les blanchisseurs d'argent font tout pour couvrir leurs traces. Leur méthode habituelle consiste à cacher leur comportement et leur identité en utilisant de faux noms (appelés « identités synthétiques »), de fausses adresses et/ou des sociétés-écrans pour accéder au système financier par l'intermédiaire de plusieurs comptes pour éviter qu'une enquête ne soit lancée par une banque ou un gouvernement.

La plupart de ces fraudes aboutissent, car les systèmes de surveillance des transactions ne sont pas bien équipés pour identifier ces tactiques. Les TMS sont habituellement basés sur des règles et ces règles sont déclenchées par des données. « Si ces données présentent des erreurs, qu'elles soient délibérées ou accidentelles, les alertes générées sont erronées. De plus, c'est précisément en raison de ces données erronées que les activités frauduleuses passent totalement inaperçues. Les banques doivent tout faire pour veiller à la fiabilité des données qui circulent dans le TMS », explique Doug Stevenson. Il précise : « L'idée que les données ne peuvent être traitées ou corrigées qu'à leur source est fausse. En réalité, les équipes en charge de la réglementation et de la conformité disposent de technologies qui leur permettent de résoudre ces problèmes directement, quelle que soit l'origine des données. »

Comme l'explique Richard Stocks, directeur Global Solutions, Financial Crimes and Compliance chez Pitney Bowes, ce type de problème a deux conséquences principales : « La première est que le comportement frauduleux passe inaperçu et que les comportements non détectés sont considérés comme des faux négatifs. C'est ainsi que le blanchiment d'argent et le financement du terrorisme sont possibles sans que les systèmes, processus et contrôles des banques ne puissent les identifier. » Par exemple, si une seule partie transfère de l'argent par l'intermédiaire de plusieurs comptes, même de manière légale, plusieurs alertes sont générées. Si les transactions relevant du blanchiment d'argent semblent légales et ne sont pas mises en relation de manière évidente, les enquêtes qui s'ensuivent risquent de ne pas les déceler faute d'une vue d'ensemble. « C'est alors que les banques s'exposent à des amendes pour infraction à la réglementation », déclare Richard Stocks.

« La seconde conséquence est le taux de faux positifs », qui se situe entre 95 % et 98 % d'après Richard Stocks. « Cela signifie que sur 100 000 alertes, 95 000 sont négligeables et constituent une perte de temps pour les enquêteurs. »

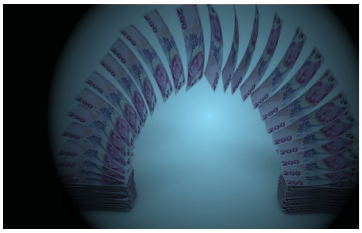
Cependant, les experts interrogés s'accordent à dire que la tentation d'incriminer le système de surveillance des transactions n'est souvent pas justifiée. « Les systèmes de surveillance des transactions

remplissent leurs fonctions », assure Michael Wilson, directeur marketing, solutions sectorielles chez Pitney Bowes Software. « Ce sont des outils fondamentaux et ils fonctionnent correctement, mais si nous les alimentons avec des données inexactes ou incorrectes, les résultats ne pourront pas être optimaux. »

Les données constituent un aspect crucial. Des données manquantes, incorrectes, mal formatées ou saisies dans des champs non appropriés compromettent la fiabilité des résultats et peuvent être à l'origine des nombreux faux positifs qui submergent les enquêteurs. Cela nécessite un effort de nettoyage, de standardisation et de validation des données saisies. Par conséquent, une adresse qui n'a pas été saisie correctement serait standardisée selon les exigences du service postal du pays, puis validée.

Ce type de paramètre de qualité des données peut se situer entre les données source (p. ex. : gestion des données de référence) et le TMS pour uniformiser le tout, comme l'explique Doug Stevenson. Un remplacement onéreux du TMS n'est donc pas nécessaire. En outre, la capacité du TMS à scruter les opérations complète la vision d'ensemble que l'approche relationnelle permet de révéler : ensemble, ils permettent de regrouper les transactions associées et de réduire les faux positifs, tout en offrant une plus grande visibilité sur les relations sous-jacentes entre les transactions et les comptes.

> *« Sur 100 000 alertes, 95 000 sont négligeables et constituent une perte de temps pour les enquêteurs. »*
>
> **—Richard Stocks**
> Directeur Global Solutions,
> Financial Crimes and Compliance,
> Pitney Bowes



INDIVIDUS, PROCESSUS ET TECHNOLOGIES : LES TROIS PILIERS DE LA CONFORMITÉ

Julie Conroy occupe le poste de directrice de recherche chez Aite Group, une société de recherche et de conseils en services financiers. Nous avons recueilli ses impressions sur certains des défis liés à la conformité et à la détection de la criminalité financière, et sur les solutions possibles. La conversation suivante a été éditée pour plus de clarté et de brièveté.

En quoi les configurations traditionnelles des systèmes de surveillance des transactions empêchent-elles la détection des fraudes financières ?

À l'heure actuelle, de nombreuses technologies de surveillance des transactions s'appuient essentiellement sur l'analyse heuristique. Elles sont basées sur des éléments que nous avons observés par le passé. Cette méthode se révèle utile pour parer à de nombreuses difficultés basiques. L'approche basée sur des règles présente toutefois une faille : les criminels parviennent rapidement à comprendre ces règles et effectuent les ajustements nécessaires pour les déjouer.

C'est pourquoi, la nouvelle génération [de solutions] s'appuie davantage sur l'intelligence artificielle et l'apprentissage automatique, qui traitent un plus large éventail de données et de comparaisons. Je pense notamment à la création de groupes de pairs à plusieurs niveaux ou à la possibilité pour une personne ou une entreprise de faire partie de plusieurs groupes de pairs et de les comparer entre eux pour tenter de détecter les anomalies.

Je pense que les institutions financières vont accorder une importance toute particulière à la façon dont elles traitent toutes ces données – tous les comportements associés aux transactions ; à savoir les transactions financières, mais aussi les interactions utilisateur (à quel moment les clients se rendent en agence, au distributeur automatique, utilisent les services bancaires en ligne, leurs appareils mobiles, envoient des SMS, tous ces paramètres) – ainsi qu'à la manière de les regrouper pour [essayer de] les comprendre.

Que doivent faire les institutions financières pour mieux détecter les fraudes ?

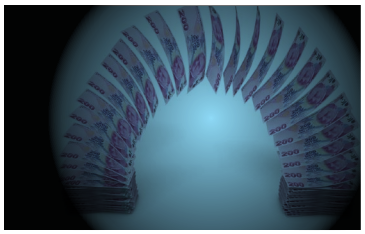
Je dirais qu'il y a plusieurs technologies adaptées et que différentes solutions sont appropriées selon le stade. La surveillance en temps réel convient pour le filtrage des listes de sanctions, mais la majorité des activités de blanchiment d'argent s'inscrivent dans un réseau de transactions et de relations au fil du temps. Partout dans le monde, l'argent peut circuler en temps réel ou presque. Dans ces situations, l'analyse en temps réel est précieuse pour les listes de sanctions et la fraude, mais l'analyse des réseaux sur la durée est indispensable pour identifier des schémas complexes de blanchiment d'argent. Il vous faut une solution capable de gérer des volumes élevés de transactions avec une très faible latence. Pour analyser des fraudes complexes comme de nombreux schémas de blanchiment d'argent, notamment pour ce qui relève du trafic d'êtres humains, de drogues et d'armes, ce ne sont pas des transactions isolées que l'on recherche, mais des tendances à bien plus grande échelle. Pour cela, il faut opter pour des méthodes orientées graphe, capables d'établir des liens entre les transactions et de les révéler aux enquêteurs.

Quelles recommandations feriez-vous aux institutions financières en matière de conformité et de lutte contre la fraude financière ?
Pour résumer, je dirais de miser sur les individus, les processus et les technologies, qui sont les trois piliers à maîtriser. Bien souvent, ce sont les individus et les processus qui sont les plus à mêmes d'assurer et d'améliorer la conformité. Si je dis cela, c'est parce que même si ces deux piliers peuvent faire l'objet de nombreuses batailles politiques, il ne s'agit généralement pas de batailles budgétaires. Il s'agit de faire les choses différemment avec les mêmes personnes.

Mon premier conseil est donc de considérer les individus et les processus comme des moyens faciles d'améliorer les choses progressivement, tout en sachant que des améliorations technologiques vont suivre. Je conseillerais ensuite d'envisager les processus comme une composante éphémère qu'il est toujours possible de modifier au fur et à mesure que les technologies et les personnes évoluent.

Votre système de surveillance des transactions, qui examine en temps réel chaque transaction, doit pouvoir s'appuyer sur un écosystème de technologies bien plus large. Il ne s'agit pas de sélectionner une seule technologie, mais de choisir celles qui sont les plus adéquates en s'assurant qu'elles se complètent. Or, c'est là où le bât blesse dans le secteur des services financiers : il est rare que ces technologies se complètent de manière efficace.

> *« Votre TMS doit pouvoir s'appuyer sur un écosystème de technologies bien plus large. »*
>
> **—Julie Conroy**
> Directrice de recherche,
> Aite Group



AU-DELÀ DES TRANSACTIONS

Rick Skriletz est responsable des données et des analyses chez RCG Global Services, un fournisseur de solutions technologiques partenaire de Pitney Bowes qui travaille dans le secteur des services financiers. Nous avons abordé avec lui l'approche relationnelle et son utilité dans le domaine de la criminalité et de la conformité financières. La conversation suivante a été éditée pour plus de clarté et de brièveté.

En quoi une approche relationnelle renforce-t-elle et améliore-t-elle l'utilisation que les institutions font déjà de leurs TMS ?

Pour moi, un système de surveillance des transactions est comparable à un microscope : il permet d'examiner précisément chaque opération. Une transaction a excédé la limite ? Le système l'examine. Une autre opération dépasse la limite ? Le système l'examine. Dans une grande institution, tous ces événements peuvent être vérifiés par des personnes différentes, même s'ils sont liés. Au-delà de cette vue microscopique qui considère chaque événement séparément, vous devez avoir une vue globale de toutes ces transactions qui sont en lien les unes avec les autres et qui constituent un ensemble. Les criminels qui se livrent au blanchiment d'argent et à la fraude connaissent les limites légales au-delà desquelles une transaction fait l'objet d'un examen. En examinant les transactions associées dans leur ensemble, vous pouvez détecter des problèmes que vous n'aviez pas décelés auparavant. Un microscope peut être utile pour certaines choses, mais vous avez besoin d'autres outils pour aborder les problèmes de manière plus globale.

Quels sont le rôle et l'importance des données dans une approche relationnelle ?

La faculté à établir les liens repose en grande partie sur la capacité à ne pas utiliser uniquement l'entrée telle qu'elle existe et qui doit rester intacte. En effet, il est important d'aller plus loin : même s'il s'agit du nom légal, d'autres indicateurs comme un numéro de téléphone, une adresse ou tout type d'historique ou d'événement me permettent-ils de déduire qu'il s'agit sûrement de la même personne ? Je peux alors étendre les relations associées à chacun de ces événements distincts, qu'il s'agisse de cosignataires sur un compte, d'un quelconque bénéficiaire ou d'une quelconque relation (fiduciaire, par exemple).

UNE APPROCHE RELATIONNELLE

Si les systèmes de surveillance des transactions cherchent à détecter les opérations frauduleuses ou les parties non autorisées en procédant transaction par transaction, l'approche relationnelle vient compléter cette démarche en offrant une vision bien plus large.

Pour ce faire, elle apporte d'autres informations connues et déductibles, dont certaines sont enrichies par des jeux de données externes, qui permettent de contextualiser les transactions, les parties impliquées et leurs relations, le tout dans le but de réduire la quantité de faux positifs et de faciliter les enquêtes tout en augmentant les taux de détection réelle. Comme l'utilisation de cette technologie se répand, il est probable que les régulateurs s'attendent à des niveaux accrus de détection de la part des institutions financières, comme le suggère Rob Mara d'Ernst & Young (voir l'entretien page 14).

L'approche relationnelle offre quelques avantages majeurs :

- **Réduction du nombre de faux positifs :** grâce à un regroupement des alertes connexes et à l'identification des transactions légales (p. ex. : paiement de frais de scolarité ou acompte pour un prêt hypothécaire).
- **Amélioration de la détection des faux négatifs :** en identifiant des relations sous-jacentes entre les comptes, il est possible d'établir un lien entre les transactions qui n'ont aucun lien apparent et qui sont en dessous du seuil. De plus, comme l'identité des titulaires de compte est plus facile à déterminer, le risque d'effectuer des transactions avec une personne liée à des parties non autorisées est moindre.
- **Simplification des enquêtes :** que l'alerte générée soit erronée ou justifiée, l'enquête est facilitée par les relations et les données contextuelles, ainsi que par des indications visuelles qui permettent aux agents de conformité de déterminer rapidement si une transaction est légale.
- **Réduction des coûts globaux :** avec un nombre réduit de faux positifs et la simplification des enquêtes, les agents de conformité peuvent consacrer moins de temps et de ressources au suivi, ce qui permet aux institutions financières de réaffecter les ressources des services de conformité.

La base de données graphe est au cœur de cette approche relationnelle. Contrairement à une base de données relationnelle classique qui stocke les informations dans des tables et colonnes séparées et nécessite un code compliqué pour joindre les données connexes et établir des liens, la base de données graphe stocke les informations en tant que « nœuds » et « relations ». Par exemple, un client peut être représenté par un nœud relié à d'autres nœuds, comme des entreprises, à l'aide de lignes qui indiquent la nature de la relation (p. ex. : collaborateur, propriétaire ou autre). Utpal Bhatt, vice-président du marketing chez Neo Technology, éditeur de la solution Neo4j, l'une des bases de données graphe les plus populaires du secteur (voir l'entretien page 13), explique : « En clair, les [bases de données graphe] stockent les données sous leur forme naturelle, en tant que jeu de données composé de nœuds et de relations. »

« Les transactions essaient de vous raconter une histoire. Êtes-vous à l'écoute ? »

—Doug Stevenson
Directeur général,
Global Financial Crimes and Compliance,
Pitney Bowes

Il poursuit : « Même s'il ne constitue pas une solution miracle, le graphe est un outil très puissant capable de lutter contre ces nouveaux types de fraudes. Et il ne fait pas que les combattre. Il peut empêcher qu'elles ne se produisent. Grâce aux bases de données graphe, il est possible d'anticiper et de prédire le comportement probable d'une entité. C'est pourquoi je pense qu'il s'agit d'un investissement technologique primordial pour les sociétés de services financiers. »

Cela permet à la technologie utilisant les bases de données graphe d'effectuer un certain nombre de tâches utiles, comme identifier et regrouper les alertes similaires et mettre en évidence des relations qu'un TMS n'aurait pas décelées (le fait que Jean, J.P. et Jean-Paul Dupont sont la même personne, par exemple).

« L'analyse des relations permet de commencer à identifier des tendances qui, une fois groupées, peuvent révéler des schémas de transactions spécifiques, explique Rick Skriletz de RCG Global Services. Vous pouvez ensuite les mettre en relation avec certains éléments et comportements, comme des tailles de transactions similaires, des adresses ou zones géographiques similaires, ou encore des fournisseurs ou types de fournisseurs en commun. Ce type d'informations peut vous permettre d'anticiper et de déterminer si un compte doit être surveillé. Et si les transactions commencent à excéder [les seuils], surveillez-les de très près pour vous assurer qu'il ne s'agit pas d'une fraude. »

Si les bases graphe impliquent un niveau de tolérance à l'égard des données (voir l'entretien avec Utpal Bhatt, page 13), le succès des analyses repose toujours en grande partie sur la qualité des données saisies. Il est donc essentiel de mettre en œuvre le type d'initiative mentionnée dans la précédente rubrique, qui constitue la base de l'approche relationnelle (Ne blâmons pas les TMS, page 4). Combinée à une initiative rigoureuse de qualité des données, la base de données graphe permet de relier de multiples transactions et comptes aux parties responsables et, par conséquent, elle joue un rôle central dans l'approche relationnelle. Les bases de données graphe permettent aux institutions financières de réduire les fausses alertes, et ainsi de réaliser des économies de personnel, de diminuer le coût des enquêtes et d'améliorer la conformité en général. Ce processus comporte trois étapes clés : rechercher, relier et visualiser.

RECHERCHER

Il arrive souvent que les institutions financières disposent d'un environnement logiciel imparfait, avec plusieurs systèmes – datant pour certains des années 1970 et 1980 – dans différents secteurs d'activités : la qualité des données est alors compromise. Au fil des ans, un même client peut avoir des comptes sous différentes variantes de ses nom, adresse et autres informations personnelles. Lorsqu'une partie dissimule délibérément son identité, le nombre de comptes et de variantes augmentent encore davantage. Or, une approche relationnelle associée à une initiative de qualité des données rigoureuse résout ces problèmes : l'emplacement des données n'a presque plus aucune importance. Les données peuvent être localisées et recueillies quel que soit l'endroit où elles sont stockées, que ce soit en ligne ou hors ligne, et les données dites « libres » (voir l'encadré page 12) sont extraites pour les enrichir. De plus, les données peuvent être facilement retrouvées grâce aux fonctionnalités de recherche en langage naturel et de saisie semi-automatique, qui permettent la compréhension du langage et la prédiction de requêtes comme lors d'une recherche Google.

RELIER

Même les transactions légales peuvent déclencher plusieurs alertes si l'argent transite par plusieurs comptes avant d'atteindre sa destination (p. ex. : retrait d'argent, puis transfert vers un compte courant et achat d'un montant élevé). Encore une fois, le problème s'aggrave lorsque les parties impliquées dissimulent volontairement leur identité et la

somme d'argent impliquée. « Et si vous pouviez relier toutes ces transactions ? », demande Jim Burnick de Pitney Bowes. « Et si pouviez déterminer que ces 30 ou 40 transactions en dessous du seuil émanaient de la même source ? Ou d'un numéro de téléphone associé à des noms similaires, ou encore de zones géographiques ou d'adresses IP similaires ? Vous seriez alors en mesure d'identifier un comportement suspect qui doit absolument faire l'objet d'une enquête. »

Parce qu'une vision globale met en évidence les relations, il est possible d'identifier des liens entre les comptes, même par des moyens peu évidents comme l'adresse IP ou des noms si proches qu'ils désignent vraisemblablement la même personne, comme Jim Burnick le suggère. Cette approche permet aux enquêteurs d'identifier plus facilement des réseaux d'utilisateurs. Combinées, ces mesures permettent aux agents de conformité de rechercher simultanément des groupes de transactions associées, au lieu que des enquêteurs étudient les éléments séparément ; nous sommes ainsi sûrs que les conclusions tirées à partir de ces données sont établies dans le contexte approprié.

VISUALISER

Pour faciliter les enquêtes, un outil de visualisation illustre les relations et les informations client associées sous forme de réseau de relations. Jim Burnick apprécie l'aspect « interactif » de cet outil : les utilisateurs peuvent naviguer dans le réseau « pour voir qui ou quelle entreprise est au centre du réseau, et quelle personne ou entreprise a une influence sur ce réseau de relations. Cela permet d'enquêter très efficacement sur ces scénarios de criminalité financière. »

Michael Wilson de Pitney Bowes décrit la manière dont cette structure aide les enquêteurs : « Chaque client ou partie type est semblable à une étoile. Si une partie est impliquée dans une activité suspecte, elle prend la forme d'une constellation. La capacité à trier les alertes visuellement permet aux enquêteurs de gagner un temps considérable », ajoute-t-il.

L'outil de visualisation offre également une fonction de recherche en langage naturel, avec une construction dynamique des requêtes au fur et à mesure de la saisie de l'utilisateur, tout comme Google construit et prédit les requêtes à partir d'une entrée en langage naturel.

Exploiter au mieux les données « libres »

« Les systèmes bancaires centraux et les informations qui circulent dans une banque au quotidien sont une véritable mine de renseignements, au même titre que les transactions », commente Doug Stevenson de Pitney Bowes. « Elles essaient de vous raconter une histoire. Êtes-vous à l'écoute ? »

Doug Stevenson fait référence au volume considérable d'informations contenues dans les chèques, les demandes de prêt, les permis de conduire et autres documents que la banque a déjà en sa possession, mais dont elle ne se sert jamais. Ces données, figurant sur le coupon d'un chèque, sur le scan d'un passeport ou cachées dans les détails d'un virement bancaire, par exemple, peuvent s'avérer très précieuses pour contextualiser les clients et leurs relations. En revanche, la plupart du temps, elles passent inaperçues et restent inexploitées, ce qui leur vaut le nom de « données libres » (ou données cachées).

Cependant, il est aujourd'hui possible d'extraire les données libres et de les utiliser pour identifier d'éventuels problèmes de fraude et de conformité. Ainsi, un même numéro de permis de conduire utilisé sur plusieurs permis éveille le doute sur la légalité des transactions qui y sont associées. Doug Stevenson souligne que les informations relatives aux adresses peuvent être utilisées pour effectuer des vérifications croisées avec les adresses connues pour les personnes mal intentionnées ou les pays non autorisés. « Toutes ces données, [les institutions financières] les ont à disposition, mais elles ne pouvaient jusqu'à présent pas [les utiliser] pour la simple raison que la technologie ne le leur permettait pas », précise-t-il. « La raison souvent invoquée est que cela est moins contraignant pour les banques de s'adresser à l'un de leurs fournisseurs de données (comme nous) pour obtenir ces informations, même si elles en possèdent [déjà] une grande partie dans leurs propres systèmes. »

En définitive, si l'on combine une approche relationnelle rigoureuse en matière de lutte contre le blanchiment d'argent à une technologie d'extraction de texte, ces données libres fournissent un contexte supplémentaire extrêmement précieux en permettant d'associer des comptes sans lien apparent et d'évaluer la légitimité des alertes.

RÉVÉLER DES LIENS GRÂCE AUX BASES DE DONNÉES GRAPHE

Neo Technology est l'éditeur de logiciels en charge de développer Neo4j, l'un des systèmes de base de données graphe les plus populaires du secteur, utilisé de manière notable par le Consortium international des journalistes d'investigation (ICIJ) pour démêler les relations complexes cachées derrière les sociétés-écrans dans le cadre de l'enquête sur les « Panama Papers ».[6] *Neo4j est également un composant de la solution de conformité et de lutte contre la criminalité financière de Pitney Bowes. Nous nous sommes adressés à Utpal Bhatt, vice-président du marketing chez Neo Technology, pour mieux comprendre les bases de données graphe et leurs atouts. La conversation suivante a été éditée pour plus de clarté et de brièveté.*

Comment décririez-vous et résumeriez-vous une base de données graphe à un non-spécialiste ?

La technologie consiste essentiellement en une base de données qui stocke au même niveau à la fois les données et les relations qui existent entre chaque point de donnée comme objets de première classe. Il est ainsi possible d'extraire de la valeur, non seulement des données, mais aussi de la manière dont [les points de données sont] liés les uns aux autres.

Pensez au monde dans lequel nous vivons, et en particulier dans le contexte des entreprises, où chaque ressource ou chaque information peut être liée : qu'il s'agisse d'informations sur le client ou sur le produit, d'informations sur les appareils ou de données géographiques. En termes mathématiques, cela s'appelle un graphe. Ainsi, lorsque vous stockez toutes ces informations, au lieu de les répartir en tables et colonnes et de tenter de les réassembler, la base de données graphe stocke les informations telles qu'elles existent dans la réalité. L'avantage est qu'en plus de pouvoir visualiser ces informations, vous pouvez également les parcourir rapidement d'un point à l'autre.

En quoi une base de données graphe est-elle particulièrement adaptée pour identifier les activités potentielles de blanchiment d'argent ?

Les bases de données graphes offrent deux principaux avantages dans la lutte contre la criminalité financière. Le premier est de pouvoir attribuer une note [de risque] à une personne. Nous avons écrit un article intéressant à ce sujet (« What Can The Banks Learn From Online Dating? »)[7]. L'idée est que n'importe qui peut créer un profil sur un réseau social. Toutefois, pour savoir si cette personne est réelle et si ce qu'elle dit est réel, il faut rechercher d'autres informations à son sujet : avec qui est-elle en contact et ces personnes sont-elles réelles ? Ce type de liens entre les informations va au-delà de l'individu et tient compte de la relation entre l'individu et son adresse et ses amis pour déterminer l'authenticité de son profil.

Il en va de même pour les services financiers. Que vous souscriviez une carte de crédit en ligne ou que vous fassiez une demande de prêt, il y a un degré de risque inhérent à chaque personne avec laquelle vous effectuez une transaction. Afin de limiter ce risque, vous devez enrichir les informations à l'aide d'autres données, en essayant de les compiler pour définir une note globale. C'est là qu'une base de données graphe est particulièrement utile : non seulement les relations sont stockées dans la base de données graphe, mais vous pouvez aussi les utiliser pour calculer une note quasiment en temps réel.

6 Hunger M. & Lyon W. (2016). Analysing the Panama Papers with Neo4j: Data Models, Queries & More. Extrait le 23 novembre 2016 de https://neo4j.com/blog/analyzing- panama-papers-neo4j/
7 Eifrem E. (août 2014). What Can the Banks Learn From Online Dating? Extrait le 23 novembre 2016 de https://www.wired.com/insights/2014/08/can-banks-learn-online-dating/

Le second avantage de ces bases de données est qu'elles aident les institutions à identifier les relations ou les collusions. Par exemple, un graphe est capable de détecter immédiatement qu'un numéro de sécurité sociale est associé à trois noms différents et qu'une même adresse est utilisée par quatre personnes, et que tous ont participé à une fraude. Seule une technologie comme la base de données graphe permet d'analyser les liens entre les entités, car pour comprendre la situation, il peut être nécessaire de remonter jusqu'à trois, quatre ou cinq niveaux, et les attributs à mettre en relation sont vraiment nombreux. C'est pour toutes ces raisons que Neo4j a joué un rôle clé dans l'enquête sur les « Panama Papers ». Par le passé, [l'ICIJ] aurait eu à compiler les documents manuellement à l'aide de feuilles de calcul Excel.

La qualité des données revient très souvent dans les discussions autour de ces questions. Quelle est son importance pour les bases de données graphe ?

La qualité des données stockées dans la base de données reste primordiale à tout moment. Cependant, lorsque le thème de la qualité des données est abordé, il est souvent question des contraintes imposées par d'autres modèles. Prenons l'exemple d'une société comme Neo Technology. Selon le cas, le représentant commercial va écrire Neo Tech, simplement Neo, ou encore Neo Technology. Si l'on entre ces informations dans une base de données non orientée graphe, il sera impossible de relier les trois. De ce point de vue, une base de données graphe est bien plus adaptée, car vous pouvez facilement établir un lien entre les trois entités et déterminer qu'il s'agit de la même société.

Je résumerais la qualité des données à cette évidence : « plus la qualité des données est élevée, plus vous obtenez des informations et des résultats pertinents ». Une base de données graphe est beaucoup plus flexible que les structures de données classiques pour s'adapter à ce type d'incohérences qui existeront toujours.

OBTENIR UNE VISION GLOBALE

Rob Mara dirige le service Regulatory Compliance Technology Practice chez Ernst & Young. EY et Pitney Bowes se sont associées pour développer des solutions d'analytique et de données destinées à accroître l'efficacité des programmes de lutte contre le blanchiment d'argent et de conformité aux sanctions économiques. La conversation suivante a été éditée pour plus de clarté et de brièveté.

En quoi la technologie peut-elle aider les institutions financières à résoudre ou à atténuer certaines des difficultés rencontrées dans le domaine de la détection du blanchiment d'argent et de la criminalité financière ?

Tout d'abord, même si vos données sont de mauvaise qualité, vous avez de bonnes chances de modifier et d'améliorer certaines d'entre elles, comme les adresses, en utilisant les différents types d'analyses qui existent actuellement. Les adresses sont un élément bien connu, et si vous disposez de données réelles qui permettent d'identifier ce à quoi elles correspondent, vous pouvez alors les standardiser pour savoir, par exemple, si une adresse correspond à un terrain vague, une boîte postale, etc. La technologie et l'analytique sont donc mieux à même d'améliorer les données de mauvaise qualité.

L'autre aspect qui entre en jeu est une approche basée sur l'analyse de schémas plus larges. Il ne s'agit plus simplement d'être informé lorsqu'une personne dépose 9 000 euros en espèces, mais de pouvoir détecter si un dépôt de 1 000 euros en espèces a été effectué neuf fois. Il s'agit de pouvoir identifier des tendances de manière plus large ou de comprendre les interactions grâce à l'analyse des données. [Reconnaître] les comportements comme les divisions ou les fusions permet

de détecter un éventuel événement inhabituel. Vous pouvez vous interroger : « Quinze de mes clients ont transféré de l'argent vers la même entité en dehors de ma banque. Que savons-nous de cette entité ? »

Si vous parvenez à repérer ces types de comportements au lieu de vous appuyer sur un ensemble de règles prédéfinies, et si vous pouvez améliorer les données, les incrémenter et les analyser en pensant davantage en termes de comportements et de tendances d'activités, alors vous pouvez commencer à adopter une vision prédictive et à mieux comprendre le risque auquel votre entreprise est exposée. Vous avez alors le choix entre mettre en place des contrôles plus efficaces au préalable pour éviter ce risque, ou améliorer votre travail d'identification au moment où ces activités se produisent pour barrer la route aux criminels.

Pensez-vous que les régulateurs vont s'attendre à ce que les institutions disposent de ces nouvelles technologies pour détecter le blanchiment d'argent ?

Je pense qu'avec le temps, alors que les choses évoluent à la fois sur le plan réglementaire et sur le plan de la compétitivité et des coûts, des systèmes plus performants seront nécessaires. Les régulateurs vont exiger toujours plus des banques et des autres institutions financières afin qu'elles améliorent leurs systèmes et utilisent un ensemble d'outils analytiques bien plus perfectionnés qu'auparavant.

Quel conseil donneriez-vous aux institutions qui cherchent à améliorer leur conformité dans ce domaine ?

J'aborde plusieurs points avec mes clients. Tout d'abord, d'un point de vue technologique, ils doivent penser aux capacités dont ils souhaitent bénéficier à l'avenir plutôt que de chercher à résoudre leurs problèmes immédiats. Il ne s'agit pas tant d'acheter un système basé sur des règles qui va effectuer telle et telle action, que de se poser la question : « Comment puis-je bénéficier d'analyses qui vont m'aider à découvrir des choses que j'ignore ? ». Pensez aux capacités dont vous souhaitez disposer plutôt qu'à des solutions ponctuelles.

Il convient par ailleurs d'adopter une approche globale en matière de conformité. Tout d'abord, en particulier dans le cadre de la lutte contre le blanchiment d'argent, au lieu de considérer la connaissance client (KYC), l'évaluation des risques et tous les aspects comme des éléments séparés, il faut penser à la manière dont ils sont liés les uns aux autres. En les traitant comme des éléments séparés, vous faites fausse route et vous ne gérez pas réellement les risques. Avec une telle approche, dans laquelle les différents aspects ne sont pas liés, vous consacrez beaucoup de temps et d'argent à explorer de mauvaises pistes.

Une série d'événements peut avoir de multiples implications en matière de conformité, et si vous les considérez comme des événements indépendants, vous pouvez passer à côté de l'essentiel. Et sans la technologie adéquate, il est impossible d'obtenir une vision d'ensemble.

Points clés et conseils

Les experts interrogés livrent leurs meilleurs conseils à ceux qui envisagent de mettre à niveau leurs programmes de conformité en matière de lutte contre le blanchiment d'argent et d'identification des parties non autorisées.

- **La vision que vous avez n'est pas forcément celle qu'il vous faut.** Associer les identités des clients et les relations entre les transactions peut faire penser à la « vue client unique », mais ce terme fait davantage penser au marketing qu'à la conformité. Cela pose problème lorsqu'il est question de mettre en œuvre des projets de gestion des données de référence, car la « vue » marketing n'est pas suffisante pour assurer la conformité. D'après Michael Wilson, les équipes de conformité ne doivent pas hésiter à demander davantage d'informations si le service informatique affirme qu'il dispose déjà d'une vue unique : « Creusez un peu plus loin et vérifiez si les données qui alimentent votre TMS sont réellement optimisées pour détecter les activités suspectes. »

- **Commencez par examiner les données, et non par remplacer votre TMS.** Le TMS n'est performant que s'il est alimenté par des données de qualité. « Avant de mettre en cause les outils dont vous disposez, examinez vos données », conseille Richard Stocks. « C'est là que les problèmes se situent réellement. » Avant de lancer un appel d'offres pour un nouveau TMS ou un nouvel outil de gestion des dossiers, recherchez des solutions adaptées à vos systèmes pour consolider les entités derrière les transactions selon une nouvelle approche.

- **Adoptez une approche globale, et non cloisonnée.** Cela vaut en interne comme en externe. Optez pour une vision globale des transactions et des relations entre les clients en vous aidant d'une base de données graphe pour cartographier ces relations naturellement.

De même, les processus internes relatifs à la connaissance client (KYC), à la lutte contre le blanchiment d'argent et à la surveillance des transactions ou l'évaluation des risques ne doivent pas être traités séparément. Rob Mara préconise plutôt de s'intéresser à la manière dont ils sont liés. « En les traitant comme des éléments séparés, vous faites fausse route et vous ne gérez pas réellement les risques », prévient-il. L'approche globale s'applique également à l'ensemble des domaines de la conformité, avec beaucoup de chevauchements entre les domaines réglementaires. « Une série d'événements peut avoir de multiples implications en matière de conformité, et si vous les considérez

comme des événements indépendants, vous pouvez passer à côté de l'essentiel », explique Rob Mara. « Et sans la technologie adéquate, il est impossible d'obtenir cette vision d'ensemble. » En outre, en ce qui concerne l'achat de technologies, il recommande d'anticiper l'évolution des besoins afin de trouver une solution à même d'évoluer en conséquence, plutôt que de mettre en œuvre une solution prescriptive pour résoudre un problème spécifique.

Cette approche vaut également pour les fournisseurs. Pour Doug Stevenson, les fournisseurs doivent comprendre la manière dont leur solution affecte l'ensemble du processus et ses « répercussions en cascade » tout au long du dispositif de lutte contre le blanchiment d'argent. « Si vous parlez à un fournisseur qui n'est pas en mesure de l'expliquer, j'aurais tendance à vous dire qu'il ne comprend pas le problème. Alors, assurez-vous de travailler avec des gens qui comprennent réellement la situation, parlent la même langue que vous et comprennent les implications. Ne considérez pas le cycle de vie comme un ensemble d'éléments distincts, car tout est lié. »

- **Testez les solutions potentielles sur vos propres données.** « Demandez au minimum à un fournisseur potentiel de tester sa solution sur vos données, conseille Jim Burnick de Pitney Bowes. N'attendez pas 18 ou 24 mois pour que la solution soit développée », précise-t-il. Les résultats doivent être rapides, même s'il peut être plus long de déployer l'ensemble de la solution.
- **Privilégiez la transparence.** Vous devez pouvoir examiner de près chaque alerte et comprendre pourquoi elle a été émise. Tous les systèmes de surveillance et de filtrage n'offrent pas cette transparence. Alors recherchez des solutions dans lesquelles les mécanismes ne sont pas opaques.

Conclusion

Pour assurer leur conformité aux réglementations strictes en matière de lutte contre le blanchiment d'argent et de filtrage des parties non autorisées, les banques ont besoin de solutions efficaces. Sans cela, elles perdent du temps et de l'argent à enquêter sur une myriade de faux positifs tandis que les faux négatifs échappent à leur contrôle. Toutefois, en privilégiant une approche relationnelle et en se concentrant moins sur les transactions individuelles, en exploitant les bases de données graphe pour mettre en évidence les relations masquées et regrouper les alertes, les institutions peuvent réduire de manière considérable le nombre de faux positifs et identifier plus efficacement les activités suspectes réelles, malgré les tentatives de dissimulation des fraudeurs.

Les systèmes de surveillance des transactions sont à la hauteur de leurs promesses, mais sont ralentis par la mauvaise qualité des données. Pour assurer la conformité, une solution globale permet de résoudre ce problème de qualité sans qu'il soit nécessaire de remplacer les systèmes de surveillance des transactions existants. Grâce aux données, à la précision des TMS et à la capacité à clarifier les identités et à offrir une vision plus large de la situation grâce aux bases de données graphe, il est possible d'améliorer la lutte contre le blanchiment d'argent et la conformité aux sanctions.

Pour plus d'informations sur Pitney Bowes,
les « Orfèvres du Commerce »,
rendez-vous sur : pitneybowes.com/fr/industrie/services-financiers.

REMERCIEMENTS

Forbes Insights et Pitney Bowes remercient les personnes suivantes pour leur temps et leur expertise :

Utpal Bhatt, Vice-président du marketing, Neo Technology

Jim Burnick, Directeur général, Financial Services Solutions, Pitney Bowes

Julie Conroy, Directrice de recherche, Aite Group

Rob Mara, Principal, Advisory Services, Ernst & Young LLP

Rick Skriletz, Global Managing Principal, RCG Global Services

Doug Stevenson, Directeur général, Global Financial Crimes and Compliance, Pitney Bowes

Richard Stocks, Directeur Global Solutions, Financial Crimes and Compliance, Pitney Bowes

Michael Wilson, Directeur marketing, solutions sectorielles, Pitney Bowes Software

Forbes
INSIGHTS

À PROPOS DE FORBES INSIGHTS

Forbes Insights est l'institut de recherches stratégiques et de leadership d'opinion de Forbes Media, société internationale de médias, de stratégie de marque et de technologie, dont les plates-formes combinées sont utilisées chaque mois par près de 75 millions de décisionnaires du monde entier. Forbes Insights tire profit de bases de données propriétaires des hauts dirigeants de la communauté *Forbes* pour mener des recherches sur une multitude de sujets, afin de positionner les marques comme leaders visionnaires et accroître l'engagement des parties prenantes. Les résultats des recherches sont accessibles sous plusieurs formes (numérique, papier et en direct) et relayés à travers les plates-formes sociales et médias de *Forbes*.

FORBES INSIGHTS

Bruce Rogers
Chief Insights Officer

Erika Maguire
Directrice des programmes

Andrea Nishi, Chargée de projet

RÉDACTION

Kasia Wandycz Moreno, Directrice
Hugo S. Moreno, Directeur
Lynda Brendish, Auteure du rapport
Dianne Athey, Graphiste
Peter Goldman, Graphiste

RECHERCHE

Ross Gagnon, Directeur
Kimberly Kurata, Analyste
Sara Chin, Analyste de recherche

VENTES

Amérique du Nord
Brian McLeod, Directeur général
bmcleod@forbes.com
Matthew Muszala, Manager
William Thompson, Manager

EMEA

Tibor Fuchsel, Manager

APAC

Serene Lee, Directrice générale

MIX
Paper from responsible sources
FSC® C018101

499 Washington Blvd., Jersey City, NJ 07310 | 212.366.8890 | www.forbes.com/forbesinsights