**SECRETARIAT GENERAL**

**Direction de la lutte contre le blanchiment de capitaux et le financement du terrorisme**

**Service de contrôle permanent**

# Revue thématique :

# Dispositifs automatisés de surveillance des opérations en matière de LCB-FT

# Rapport

Avril 2023

# Table des matières

# SYNTHÈSE

La Direction LCB-FT de l'Autorité de contrôle prudentiel et de résolution (ACPR) a mené en 2022 une revue thématique sur les dispositifs automatisés utilisés par les organismes financiers placés sous le contrôle de l'autorité pour la mise en œuvre de leurs obligations de surveillance des opérations au regard de la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT).

L'objectif de cette revue est de dresser un état des lieux du fonctionnement et des performances des outils de surveillance des opérations sous revue. Le document ne se prononce pas sur la conformité à la réglementation des pratiques décrites. L'ACPR envisage, en collaboration avec Tracfin, d'élaborer des lignes directrices sur ce thème, qui feront l'objet d'une concertation préalable à leur adoption au sein de la Commission consultative Lutte contre le blanchiment et le financement du terrorisme, instituée par l'ACPR en application de l'article L. 612-14 du code monétaire et financier.

Deux documents ont été adressés à un échantillon composé de 36 groupes et entités individuelles couvrant la plupart des types d'organisme et lignes de métier (banque de détail et en ligne, banque privée, crédit à la consommation, banque de financement et d'investissement, services d'investissement, succursales étrangères, assurances, transmission de fonds, « fintech ») :

- un questionnaire rassemblant des éléments d'ordre qualitatif sur les outils et leur place dans les dispositifs des organismes ;
- un recueil des scénarios intégrés dans les outils en vue d'établir des typologies et de comparer leur performance.

Les réponses, collectées durant l'été 2022, montrent la situation de l'échantillon à cette date.

Les participants disposent tous d'au moins un outil de surveillance automatisé ; ils y consacrent des ressources variables (de quelques centaines de milliers d'euros à plusieurs millions). Si une majorité d'entre eux a choisi une solution de marché, on constate une légère tendance au développement d'outils internes. On note également que les participants complètent généralement ces outils par des requêtes informatiques ponctuelles ou régulières, afin de répondre à des besoins spécifiques. Malgré les apports des outils de vigilance automatisés, la surveillance humaine est loin d'être marginale et les alertes qui en sont issues aboutissent plus fréquemment à des déclarations de soupçon que les alertes automatisées. Quelle que soit la part de la surveillance automatisée, tous les participants rapportent une forte implication des équipes de conformité/sécurité financière dans les choix de paramétrage des outils.

L'usage de l'intelligence artificielle est encore peu répandu, bien qu'on note que quelques organismes de taille conséquente ont acquis ou développent actuellement des solutions reposant sur ce type de technologie. Les cas d'usage remontés par les participants concernent : (1) la priorisation/optimisation du flux d'alertes, (2) l'identification de nouvelles typologies de blanchiment, (3) l'analyse de graphes favorisant le traitement d'une alerte.

En matière de pilotage et de gouvernance, la grande majorité des participants a rédigé une procédure encadrant leur dispositif de surveillance automatisée des opérations. Dans la plupart des cas, la modification du paramétrage de l'outil, voire l'introduction d'un nouveau scénario, est du ressort final des équipes centrales de conformité incluant la LCB-FT. En outre, ce sujet est régulièrement abordé lors de comités dédiés ou plus généraux traitant de la LCB-FT.

S'agissant du fonctionnement concret des outils, la revue a mis en lumière des bonnes pratiques, telles que la couverture exhaustive des opérations et des clients et l'encadrement strict des exemptions. En

revanche, on note l'absence assez fréquente de consolidation des opérations réalisées par un même client sur ses différents comptes ou produits. En ce qui concerne la fréquence de mise en œuvre des scénarios, on relève des approches différentes qui présentent chacune des avantages et des inconvénients (ex : génération continue d'alertes avec analyse rétrospective sur une période de référence glissante ou génération d'alertes selon une périodicité prédéfinie). En outre, seule une minorité d'établissements s'est mise en capacité de bloquer automatiquement certains flux suspects (hors le cas, beaucoup plus répandu, des flux à destination ou en provenance de pays considérés à risque par l'établissement), au moyen d'outils générant des alertes en temps réel qui peuvent avoir un caractère bloquant. Cependant, dans beaucoup d'établissements, les opérations les plus à risque impliquent une intervention humaine (virements de montant élevé par exemple), de sorte que ces établissements sont à même de suspendre l'opération si nécessaire.

Tous les participants ont indiqué procéder à un suivi des performances de leurs outils, donnant lieu, le cas échéant, à une revue des scénarios utilisés ou de leur paramétrage. Les indicateurs utilisés et la formalisation de ces revues sont toutefois très variables. L'introduction de nouveaux scénarios répond en partie à cette analyse de performance, ou à des évolutions internes ou externes (nouveaux produits, publications officielles). On souligne néanmoins qu'elle résulte rarement de cas concrets de non détection d'opérations suspectes dont l'établissement aurait déterminé qu'il révèle un risque insuffisamment couvert.

L'analyse des scénarios fournis par les participants a permis de souligner la faible prévalence de scénarios dédiés à la comparaison des opérations avec les ressources des clients. La prise en compte des ressources passe par la modulation des seuils de déclenchement des scénarios. Cette analyse a notamment permis d'identifier certaines typologies de scénarios qui, quoiqu'efficaces, s'avèrent encore peu répandus :

- une vigilance spécifique sur certains risques : crypto-actifs, certains nouveaux clients, clients non-résidents ;
- la mise sous surveillance de certains clients (ayant fait l'objet d'informations défavorables, de déclaration de soupçon ou de demande des autorités) ;
- la comparaison de groupes de pairs, à savoir des clients présentant des caractéristiques similaires.

En matière de traitement des alertes, les réponses ont permis d'identifier trois types d'organisation : un modèle entièrement centralisé et deux modèles partiellement décentralisés dans lesquels les commerciaux exercent soit la première analyse des alertes, soit seulement des analyses complémentaires à la demande de la fonction centrale. Les équipes bénéficient le plus souvent d'outils d'aide à la décision, dont certains très innovants (intelligence artificielle permettant l'analyse de graphes), ainsi que d'indicateurs de priorité. Ceux-ci varient fortement d'un établissement à l'autre (ancienneté, risque couvert ou encore probabilité d'escalade en DS). On peut noter enfin que certains établissements ont fait le choix de concentrer le traitement de tout ou partie des alertes générées par leur outil dans des entités de leur groupe, souvent à l'étranger, ce qui apporte des bénéfices mais peut occasionner des difficultés, notamment en cas de différences linguistiques, institutionnelles et culturelles (différences en matière fiscale, sociale ou dans l'usage des espèces notamment).

Enfin, une majorité des participants, mais pas l'intégralité, dispose d'un plan de continuité d'activité sur les outils de surveillance automatisée des transactions.

# 1. ÉLÉMENTS GÉNÉRAUX

L'utilisation de dispositifs de surveillance automatisée est généralisée. Tous les participants ont indiqué recourir à un ou plusieurs outils de surveillance automatisée.

Une majorité de participants, y compris parmi les grands groupes, utilisent des solutions de marché. Trois prestataires sont utilisés, en tout ou en partie, par environ un tiers de l'échantillon. Les participants ont souligné que le recours à un outil externe présentait notamment l'avantage d'être un moyen indirect d'échanger les meilleurs pratiques, dans la mesure où les éditeurs intègrent des évolutions qui répondent aux demandes de correction de leurs différents clients. En revanche, il est systématiquement nécessaire de mener un double travail d'adaptation des données générées par le système d'information de l'établissement aux besoins de l'outil et d'adaptation des scénarios fournis par défaut par l'éditeur à l'activité de l'établissement. On peut à ce titre remarquer que certains participants ont fait le choix de recourir à la fois à des solutions de marché et à des outils internes, selon l'activité couverte.

Il est fréquent que plusieurs outils soient utilisés selon les spécificités des activités (par exemple, un outil pour la banque de détail et un pour les activités de banque de financement et d'investissement) ou pour cibler différents types de risques (principalement des outils permettant d'identifier des comportements à risque terroriste).

En complément, les deux tiers des participants ont indiqué procéder à des requêtes hors outils, pour des motifs variés :

- cibler des opérations ou des clients en particulier, par exemple sur les clients ayant fait l'objet d'une déclaration de soupçon, afin de vérifier si l'activité suspecte se poursuit ou non ;
- cibler certaines activités ou certaines entités ;
- déployer des contrôles internes supplémentaires ;
- mener une veille sur de nouveaux risques et tester de nouveaux scénarios ; les requêtes hors outils sont aussi utilisées dans l'attente de la pérennisation de scenarios ou dans une logique palliative ;
- gagner en réactivité en cas de menace nouvelle, comme dans le cas des sanctions prises à l'encontre de la Russie en 2022.

Les dispositifs de surveillance automatisés ne remplacent pas la vigilance humaine, sur laquelle la totalité des participants continuent à s'appuyer. Cette surveillance se traduit par des remontées collaborateurs, lorsque les chargés de clientèle identifient des comportements de nature à faire apparaître un risque en matière de BC-FT. La surveillance manuelle est loin d'être marginale, tant en quantité qu'en qualité, y compris parmi les grands acteurs. La surveillance humaine est par exemple utilisée pour cibler certains clients. Ainsi, au sein des grands groupes bancaires, la proportion des déclarations de soupçon (DS) d'origine manuelle varie mais représente toujours une proportion significative, entre le tiers et les deux tiers du nombre total de déclarations. De plus, le taux de transformation des alertes manuelles en déclarations de soupçon est relativement stable entre les grands groupes bancaires, oscillant autour de 10%, et presque systématiquement bien supérieur au taux de transformation des alertes automatiques.

**S'agissant de la volumétrie d'alertes, d'examens renforcés (ER) et de déclarations de soupçons (DS) :**

- les données communiquées sont hétérogènes et ne sont pas toujours consolidées (en particulier s'agissant des grands groupes). En effet, elles peuvent être produites : par ligne de métier, par entité, ou pour l'ensemble du groupe ;

- les taux de conversion entre alertes, ER et DS sont également hétérogènes du fait de la variété des participants, des activités concernées et des méthodologies en vigueur chez chacun d'entre eux :
  - par exemple, dans certaines entités, certaines alertes sont systématiquement traitées en ER ;
  - chez certaines filiales de groupes étrangers, les alertes sont traitées au niveau central et l'entité locale ne semble pas connaître les statistiques des différentes étapes du traitement, malgré la présence de nombreuses alertes et/ou DS ;
- malgré ces difficultés, deux éléments méritent d'être signalés :
  - le taux de transformation des alertes en ER se situe globalement entre 1 et 8%, même si certains établissements disposent de valeurs extrêmes dépassant les 70% ;
  - le taux de transformation des ER en DS se situe globalement dans une fourchette bien supérieure, aux alentours de 30%. Ce chiffre recouvre une grande disparité entre des taux élevés (de 65% à plus de 90%) pour certaines activités, et des taux très bas, en l'occurrence parmi les organismes qui ont un taux élevé de transformation des alertes en ER (cf. point précédent).

L'utilisation de l'intelligence artificielle (IA) dans la surveillance des opérations reste minoritaire. Deux tiers des participants ont déclaré ne pas y avoir recours, même si plusieurs mentionnent des expérimentations en cours ou des projets à terme.

Parmi ceux qui indiquent recourir à l'IA, l'ampleur des utilisations varie, l'usage le plus fréquent étant la priorisation des alertes au moyen d'algorithmes de *machine learning*. Deux dispositifs méritent néanmoins d'être évoqués :

- un système élimine les alertes avec faible probabilité d'escalade en examen renforcé, et des analystes procèdent régulièrement à l'examen d'un échantillon d'alertes ainsi éliminées dans le but de minimiser le risque de biais des algorithmes ;
- un système réunit un large spectre des usages théoriques de l'IA, à savoir : la résolution d'entité (technique consistant à identifier des entités identiques lorsqu'il n'existe pas d'identifiant unique entre ces entités) et l'analyse de réseaux, l'identification de schémas par comparaisons de groupes de pairs, ou encore la priorisation des alertes.

Les participants exerçant spécifiquement des activités de marché (réception-transmission d'ordres, conseil, courtage) privilégient une surveillance centrée sur la détection des infractions de marché.

# 2. GOUVERNANCE ET PILOTAGE

## 2.1. Procédures

La quasi-totalité des participants s'est dotée d'une politique ou d'une procédure globale portant sur le dispositif de surveillance des opérations, même si dans certains cas il s'agit d'une partie d'un document-cadre en matière de LCB-FT, et d'un recueil de scénarios.

## 2.2. Moyens alloués à la surveillance automatisée

Les moyens financiers consacrés par les grands groupes bancaires au fonctionnement des outils de surveillance automatisé en banque de détail sont généralement de l'ordre de 5 à 10 millions d'euros par an, sans compter les frais de développement de nouveaux outils, qui peuvent excéder 10 millions

d'euros. Pour des établissements de plus petite taille, les budgets déclarés sont inférieurs à 500 000 euros.

Pour les grands groupes d'assurance ou les filiales d'assurance de grands groupes bancaires, les moyens consacrés annuellement à la surveillance automatisée sont en général compris entre 1 et 2 millions d'euros.

S'agissant du nombre de personnes habilitées aux outils, les pratiques varient considérablement, même entre groupes comparables. Par exemple, pour la banque de détail, qui consomme le plus de ressources en matière de traitement des alertes, certains grands groupes donnent accès à leurs outils à plus de 20 000 personnes et ne sont pas en mesure d'évaluer le temps consacré au traitement des alertes. Pour d'autres, notamment 5 des 7 plus grands groupes bancaires, l'utilisation des outils est le fait de quelques centaines de personnes au sein d'unités spécialisées : entre 78 et 269 ETP sont consacrés au traitement des alertes, souvent localisés au sein de centres de traitement intra-groupe à l'étranger. Le nombre de personnes habilitées aux outils est dépendant du modèle d'organisation choisi par l'établissement, en particulier selon l'activité couverte et la répartition des rôles entre lignes de défense, et de l'architecture de ses outils (insertion du workflow de traitement des alertes dans l'outil de surveillance des transactions ou utilisation d'un outil séparé).

Pour les grandes sociétés d'assurance, qui traitent un nombre d'opérations nettement moindre, le temps consacré au traitement des alertes est généralement de l'ordre de 10 à 20 ETP.

### 2.3. Pilotage

La quasi-totalité des réponses témoigne d'une forte implication des équipes centrales (conformité, sécurité financière, LCB-FT) dans la proposition et la validation des modifications de paramétrage, qui sont ensuite mises en œuvre le plus souvent par les équipes informatiques. Au sein des grands groupes, certaines entités ou lignes métier peuvent être directement à l'initiative de ces modifications, ou détenir la faculté de les valider in fine après proposition des équipes centrales dédiées. Deux participants, dont l'un appartient à un groupe étranger, déclarent que ces modifications sont de la responsabilité directe des équipes locales de l'entité.

Une majorité des participants a indiqué que des comités de pilotage traitaient des questions relatives aux dispositifs de surveillance des opérations. En général, il s'agit de comités ayant des responsabilités plus larges dans lesquels cette thématique est abordée. Les organismes qui ne disposaient pas de tels comités étaient des entités de plus petite taille, ou bien des filiales ou succursales d'établissements étrangers.

## 3. FONCTIONNEMENT DES OUTILS ET DONNÉES UTILISÉES

### 3.1. Modalités de fonctionnement des outils

#### 3.1.1. Couverture des opérations et de la clientèle

<u>Couverture des opérations</u>

La majorité des participants affirment que leurs outils couvrent la totalité ou quasi-totalité des opérations de leur clientèle, étant précisé que la pratique générale est d'exclure un certain nombre d'opérations « techniques » (opérations entre comptes d'un même client notamment) qui généreraient du « bruit » et diminueraient la pertinence des outils. Hors cette hypothèse, les entités qui rapportent exclure certains flux le justifient :

- *pour des raisons techniques* : opérations spécifiques de faible volumétrie dans des établissements de petite taille (deux établissements ont indiqué préférer utiliser des requêtes manuelles, l'un pour la compensation de chèques, l'autre pour la correspondance bancaire), ou opérations non entièrement dématérialisées nécessitant l'intervention d'opérateurs pouvant exercer des diligences LCB-FT (trade finance) ;
- *par leur analyse des risques* : dans ce cas, l'opération est exclue de la couverture de l'outil en raison de son faible niveau de risque, la vigilance reposant alors exclusivement sur une surveillance manuelle.

Certaines opérations ne sont quasiment jamais exclues du dispositif automatisé ; quand elles le sont, des actions correctives ont été annoncées : flux cartes en banque de détail et prélèvement automatiques (SDD) ou flux internationaux par exemple.

Couverture de la clientèle

Peu de participants ont mis en place des exemptions portant sur des segments de clientèle (trois cas) ou des listes nominatives de clients exemptés (quatre). Afin de limiter le risque, ces exemptions sont analysées et revues périodiquement (annuellement en majorité).

Bien qu'il ne s'agisse pas d'une exemption à proprement parler, des exclusions de certains segments de clientèle, scénario par scénario, sont fréquents afin de limiter la couverture à une clientèle cible et d'accroître la pertinence des scénarios. Dans ce cas, la pratique majoritaire consiste à revoir ces exclusions en même temps que les règles des scénarios.

### 3.1.2. Fréquence de mise en œuvre de l'outil et caractère bloquant des alertes

La majorité des participants fait varier la fréquence de mise en œuvre selon les scénarios, en fonction du type d'opération recherché. Les fréquences les plus courantes sont 24h/une semaine/un mois. A l'exception d'un assureur, tous les participants ont au moins un scénario qui tourne à fréquence quotidienne.

Un certain nombre de participants ont introduit une approche rétrospective (« look back »), pour les scénarios reposant sur un calcul de cumul ou l'identification d'une variation par rapport à un historique. Cette méthode n'est néanmoins pas directement applicable aux nouveaux clients, en l'absence d'historique, ce qui justifie une approche particulière à leur égard.

Quelques tendances se dégagent :

- certains participants, plutôt minoritaires, n'ont que des scénarios fonctionnant quotidiennement, mais pratiquent une analyse rétrospective sur une période donnée (en général hebdomadaire ou mensuelle). Cette pratique présente l'avantage de permettre une remontée en continu d'alertes, et donc une meilleure réactivité. A l'inverse, elle peut générer un nombre excessif d'alertes dès lors que les mêmes opérations sont détectées plusieurs fois, sauf à disposer d'une solution technique de neutralisation des opérations déjà analysées ;
- certains participants utilisent des fréquences moins élevées. Ils évitent ainsi la multiplication des alertes pour une même opération, mais, de fait, perdent en réactivité et en précision (notamment en cas de fractionnement d'opérations sur deux périodes), faute d'observer les opérations en périodes glissantes.

Il est rare que la profondeur de l'analyse rétrospective soit supérieure à un mois (5 participants, dont 2 mentionnent une période annuelle). On relève également le cas d'un participant qui n'a mis en place

que des scénarios à fréquence quotidienne sans analyse rétrospective, même si cette situation est en cours de remédiation.

Un participant se distingue par un outil qui tourne à fréquence quotidienne mais n'adresse les alertes, regroupées en « cas » attachés à un client, que mensuellement aux investigateurs. Ce système s'insère dans une cinétique relativement sophistiquée, qui permet d'augmenter la pertinence des alertes en éliminant celles auxquelles est associée une faible probabilité d'escalade en DS.

Huit participants, plutôt de petite taille et rattachables au groupe des « fintech », notamment dans le domaine des services de paiement, utilisent au moins en partie des outils fonctionnant en temps réel, permettant une analyse et un blocage de l'opération avant son exécution. Hormis ces cas, les alertes bloquantes paraissent uniquement associées aux filtrages visant les risques associés à certains pays ou la mise en œuvre des dispositifs de sanctions financières ciblées (gel des avoirs). Les organismes dans lesquels les alertes bloquantes sont ainsi limitées font davantage intervenir la vigilance humaine : les opérations qui nécessitent une intervention humaine font ainsi l'objet d'une vigilance en temps réel, par exemple les virements sortants de montant important.

#### 3.1.3. Contrôle interne

La quasi-totalité des participants ont mis en place des mesures de contrôle interne sur l'injection des flux d'opération dans les outils de surveillance. On relève toutefois des natures et surtout des fréquences de contrôle hétérogènes (de quotidienne à annuelle). Les contrôles les plus fréquents sont le contrôle des écarts de volumétrie entre les données de gestion (« core banking ») et l'outil, la comparaison des données attendues et des données reçues, et le contrôle des codes opérations. Ces contrôles peuvent être automatisés ou manuels. Certains établissements ont rapporté se reposer exclusivement sur des dispositifs d'alerte directement intégrés à l'outil, mais il n'est pas certain que de tels dispositifs suffisent à s'assurer de manière indépendante que l'outil fonctionne correctement.

Les différents contrôles conduits par la deuxième ligne de défense (contrôle permanent) et par la troisième ligne de défense (inspection et audit) revêtent également une importance particulière dans le dispositif de surveillance automatisée des opérations, complétant ainsi les contrôles continus en vigueur évoqués ci-dessus.

Un prestataire de service d'investissement se distingue par la mise en place d'une modulation de la fréquence des contrôles selon une approche par les risques (annuelle pour les scénarios visant la couverture d'un risque jugé faible, semestrielle pour les risques moyens, trimestrielle pour les risques élevés).

### 3.2. Données prises en compte par les outils

#### 3.2.1. Consolidation des comptes, produits et filiales

Seuls 7 participants affirment que leur outil opère une consolidation des différents comptes et produits sur un périmètre couvrant l'ensemble de leurs filiales ; 15 participants opèrent, à l'échelle de leur périmètre individuel, une consolidation entre les différents comptes et entre les différents produits. Des participants ont relevé que la réglementation de certains pays pouvait faire obstacle à l'intégration en continu dans un même outil de vigilance d'opérations relevant d'entités situées dans des pays différents (par exemple, secret professionnel ou réglementation du traitement des données). Certains participants ont aussi noté que la pertinence et le paramétrage de certains scénarios variaient d'un pays à l'autre (par exemple, pratiques différentes dans l'utilisation des espèces).

12 participants n'opèrent pas de consolidation entre les différents comptes détenus par un même client. Pour toutes ces entités, la vision globale sur un client ne peut se faire que lors des investigations menées par les analystes si une alerte a été déclenchée.

### 3.2.2. Données relatives aux opérations et aux clients

Des données relatives au client sont en général prises en compte, au moins via le score ou niveau de risque du client. L'intégration directe de données telles que les revenus ou le chiffre d'affaires du client pour faire varier les paramètres des scénarios est plus rare dans le secteur bancaire, à l'inverse du secteur des assurances. En effet, la prise en compte directe des ressources des clients (revenu, chiffre d'affaires, patrimoine, etc.) n'est rapportée que par environ un tiers des participants, même si ces données sont susceptibles d'être utilisées lors du traitement de l'alerte. D'autres participants appliquent des scénarios différenciés par segment de clientèle pouvant refléter les niveaux de revenus ; les flux créditeurs du compte peuvent également être utilisés pour approcher le niveau de revenus. Quand les ressources sont prises en compte, différentes approches existent, notamment pour les entreprises (chiffre d'affaires, trésorerie, voire nombre de salariés). Deux participants ont rapporté ne prendre en compte aucun attribut client, mais travailler à une évolution.

D'autres informations relatives aux opérations ou aux clients sont cependant parfois prises en compte directement dans les scénarios. Ces attributs n'ont été mentionnés en général que par un ou deux participants et sont spécifiques à certains modèles d'affaires (crédit, assurances) :

- *Flux* : le fait que l'opération soit réalisée à distance ou non ; la nature du distributeur ; un changement de clause bénéficiaire ; un changement de RIB/IBAN ;
- *Attributs client* : l'existence d'une procuration sur le compte ou d'une mesure de protection juridique ; l'indicateur récalcitrant FATCA/CRS ; l'ancienneté de la relation d'affaires ; l'âge du client ; des sinistres ou rachats précoces ; un train de vie incohérent avec la connaissance client ; le respect d'un taux d'endettement maximum et schéma délégataire permettant d'assurer une cohérence entre le montant financé, les revenus déclarés du client et le montant de la mensualité ; des situations à risque relevant du comportement du client ou prospect (par exemple : présence d'un impayé dans les 3 mois suivants la mise en place du dossier, cession d'un véhicule à un tiers, etc.) et laissant apparaître une incohérence à la fois de l'opération et du fonctionnement du dossier de crédit ; l'adresse de résidence ; la mention NPAI ; la typologie du client (clients en risque faible, par exemple les assureurs et OPCVM).

Il est probable qu'un plus grand nombre d'organismes intègrent certains de ces facteurs dans la détermination du risque associé au client, et que ces facteurs soient ainsi pris en compte dans les scénarios.

Rares sont les participants à considérer les modalités de connexion à leur système d'information comme un critère d'alerte, même si plusieurs y travaillent. D'autres, sans en faire un critère d'alerte, disposent de la donnée pour les investigations de leurs analystes.

Une courte majorité de participants répond ne pas prendre en compte les tentatives d'opérations/opérations annulées (ce qui est en partie expliqué par les modalités d'injection des données dans l'outil, qui se fait post exécution). On peut noter le cas d'un transmetteur de fonds qui a une politique d'examen systématique de certaines annulations (« *cancelled suspicious* »), et celui d'un établissement de crédit qui analyse les opérations annulées dans le cadre du filtrage sanction. Cela permet ainsi de satisfaire le cas échéant à l'obligation déclaration de soupçon, qui porte aussi sur les tentatives d'opérations (V de l'article L. 561-15 du Code monétaire et financier).

Le questionnaire interrogeait sur la façon dont était opérée la vigilance sur des clients liés (conjoints, plus largement groupe familial, bénéficiaires effectifs, mandataires, dirigeants, sociétés d'un même groupe, etc.). Il apparaît que la prise en compte des liens entre les clients se fait majoritairement par les investigations des analystes et/ou via le score LCB-FT (règles de contagion), et non directement dans le cadre de la surveillance automatique des opérations. On note une exception, qui dispose de seuils spécifiques pour les clients faisant partie d'un même « foyer » (notion qui englobe notamment les partenaires d'affaires).

#### 3.2.3. Liste pays

La quasi-totalité des entités interrogées ont affirmé utiliser, pour leur outil de surveillance, la dernière liste à jour des pays à risque qu'ils ont identifiés dans le cadre de leur classification des risques (axe pays).

On note toutefois que deux participants répondent par la négative, dont l'un parce qu'il n'a mis en place aucun scénario relatif aux pays à risque (scénario « non résident » uniquement). Un seul établissement ne répond pas directement, en indiquant qu'il ne gère que des paiements SEPA.

# 4. SUIVI DE LA PERFORMANCE DES OUTILS

## 4.1. Tests préalables à la mise en place de scénarios

Les tests effectués avant la mise en place de scénarios et leur *back-testing* ainsi que celui de leurs paramétrages consistent globalement à vérifier la pertinence des seuils paramétrés dans les scénarios, au regard notamment du profil de risque client et des mouvements sur les comptes.

Les indicateurs qui concourent à la décision ou non de mettre en place un scénario sont dans l'ensemble les mêmes que ceux intervenant dans le suivi des performances des scénarios (cf. infra).

Les équipes métiers travaillent étroitement avec les équipes techniques, de pilotage, et opérationnelles lors de la phase de conduite de tests de pertinence et de volumétrie dans le but d'effectuer des ajustements/recalibrages le cas échéant.

## 4.2. Indicateurs de performance des scénarios

La plupart des participants ont élaboré des indicateurs de suivi des performances des scénarios. Parmi les indicateurs les plus répandus figurent notamment :

- le volume d'alertes générées par chaque scénario ;
- le taux de transformation, par scénario, des alertes en examens renforcés ;
- le taux de transformation, par scénario, des alertes en déclarations de soupçons ;
- le délai moyen de traitement des alertes engendrées par chaque scénario.

Certains participants ont adopté des indicateurs de suivi plus fins tels que :

- la fréquence d'intervention des scénarios dans le score d'une alerte (en nombre et en pourcentage) ;
- l'analyse des flux se trouvant sous le seuil, pour en vérifier la pertinence ;
- le taux de conversion du scénario/de l'alerte en aggravation du score de risque du client.

Un participant a établi des indicateurs différents en fonction de la typologie des alertes (alerte déclenchée par une opération unique ; alerte déclenchée par une série d'opérations ; alerte comportementale).

Le suivi des indicateurs a pour but d'engager le plus rapidement possible une ou plusieurs actions correctrices en cas de détection d'une anomalie dans le dispositif de surveillance automatisée des opérations.

### 4.3. Fréquence de revue des scénarios

La fréquence de revue des scénarios, englobant le plus souvent la revue de leur paramétrage, est a minima annuelle chez la plupart des participants. Quelques participants appliquent une revue tous les deux ans. Un organisme spécialisé dans les paiements internationaux applique une fréquence de revue des scénarios fixée à trois mois. Certains n'ont défini aucune fréquence minimale de revue des scénarios.

Un participant faisant partie d'un groupe international avec un grand nombre de lignes métiers détermine la fréquence de revue d'un scénario en fonction du risque qu'il lui associe : 5 ans pour les scénarios à risque « très faible » et « faible » ; 3 ans pour les « moyen » ; et 2 ans pour les « risqué » et « très risqué ». Ce même organisme suit en outre les indicateurs des performances des scénarios en fonction du risque associé à chaque scénario : fréquence trimestrielle pour les « risqué » et « très risqué », semestrielle pour les « moyen », et enfin, annuelle pour les « très faible » et « faible ».

Enfin, un organisme a mis en place un suivi journalier des performances des scénarios, celui-ci étant directement intégré dans l'outil récemment déployé.

Dans l'ensemble, les participants indiquent suivre de façon continue les performances des scénarios paramétrés dans leur(s) outil(s) de surveillance automatisée.

### 4.4. Critères de modification des scénarios existants et d'introduction de nouveaux scénarios

Les experts métier qui traitent les alertes au jour le jour sont les mieux placés pour identifier les besoins d'évolution des scénarios et de leurs paramétrages. Par ailleurs, des événements déclencheurs, de différente nature, sont susceptibles de conduire à une révision de l'ensemble de scénarios ou de seulement certains d'entre eux :

- l'élément déclencheur le plus fréquemment mentionné est le déploiement de nouveaux produits/services et corrélativement l'identification de nouvelles typologies de risques BC-FT dans les produits/services. Peut également s'y rattacher un changement de politique commerciale conduisant à des changements profonds de typologie de la clientèle ;
- des informations émanant de publications officielles (rapport de Tracfin, rapport de *Transparency International* sur le niveau de corruption par pays, etc.) susceptibles d'évoquer de nouvelles typologies ou nouveaux risques BC-FT ;
- de nouvelles exigences réglementaires LCB-FT, des échanges avec les régulateurs, ou encore les suites d'un contrôle sur place ;
- un audit interne ;
- des évolutions dans le dispositif LCB-FT (exemples : nouvelle politique LCB-FT ou classification des risques, nouvelle segmentation de la clientèle, évolution du processus d'entrée en relation) ;
- des comparatifs de scénarios entre entités au sein d'un même groupe.

Enfin, dans le cadre du suivi des indicateurs de performance des scénarios (cf. supra), le dépassement de certains seuils prédéfinis est susceptible de conduire à une revue des scénarios ou à une révision de leur paramétrage.

Du fait de la mise en place d'une révision a minima annuelle de leurs scénarios, la quasi-totalité des participants introduisent régulièrement de nouveaux scénarios. Parmi les nouveaux scénarios récemment introduits, certaines typologies sont communes à plusieurs participants. Par exemple, on note une tendance à l'amélioration des scénarios concernant les transferts de fonds avec l'étranger, avec par exemple la prise en compte de facteurs tels que le lien du client avec le pays étranger concerné (par exemple, résidence fiscale) ou une prise en compte plus fine du risque pays (par exemple, pays avec un risque élevé de trafic de stupéfiants pour la transmission de fonds).

Parmi les évolutions récentes, les risques suivants apparaissent également dans les réponses de plusieurs participants : comptes dormants, associations cultuelles, virement à destination de personnes incarcérées. La vigilance à l'égard de ces derniers est désormais répandue dans les grands groupes, à la suite des alertes diffusées par les autorités.

Eu égard aux activités de correspondance bancaire, quelques participants ont récemment introduit de nouveaux scénarios à la suite du développement de cette activité. Plusieurs participants ont introduit des dispositifs ciblant particulièrement le trading de cryptoactifs, qui visent les paiements des clients en direction ou en provenance de ces plateformes. Ils s'appuient dans la majorité des cas sur une liste d'IBAN. Aucun établissement ne précise effectuer des requêtes a priori sur des recherches textuelles ("crypto", "bitcoin", "coin", etc.).

Un établissement a rapporté la création d'un scénario à partir d'un cas concret d'absence de détection d'opérations suspectes (découvertes après coup à la suite d'échanges avec la police judiciaire).

Certains participants n'ont pas introduit récemment de nouveaux scénarios. Un seul participant déclare avoir procédé à la suppression de plusieurs scénarios lors de la dernière revue, cette dernière ayant révélé chez certains d'entre eux un manque de pertinence ou un risque déjà couvert par d'autres scénarios.

Les contrôles de l'ACPR montrent que des incertitudes stratégiques (projet de cession d'une activité ou de l'ensemble de l'entité) peuvent conduire à un ralentissement voire une interruption dommageable de la maintenance ou des évolutions de l'outil de surveillance. Il se peut aussi qu'un renouvellement complet de l'outil soit nécessaire, par exemple à la suite de faiblesses relevées par l'audit interne ou un contrôle de l'ACPR : cette phase de transition est un moment sensible, car l'établissement doit à la fois continuer à utiliser l'ancien outil tout en investissant dans un nouvel outil.

### 4.5. Intelligence artificielle (IA)

Plusieurs participants, les grands groupes notamment, commencent à recourir à l'IA dans le cadre de la surveillance automatisée des opérations tandis que d'autres, souvent de moindre taille et disposant de moins de moyens, envisagent cette possibilité.

En effet, ces participants utilisent notamment l'IA pour : (i) appréhender les profils comportementaux des clients, (ii) prioriser le traitement des alertes, voire écarter de façon automatisée les alertes considérées comme non pertinentes sur la base de données historiques, et enfin, (iii) mettre à disposition des experts des outils d'analyse de graphe pour le traitement des alertes.

Par exemple, deux participants conduisent actuellement des tests dans le but de mieux calibrer l'adéquation entre alertes générées et pertinence du paramétrage des scénarios.

# 5. TRAITEMENT DES ALERTES

## 5.1. Éléments généraux

Le traitement par différents niveaux (jusqu'à trois niveaux) est une pratique fréquente. Au regard des éléments fournis, trois circuits de traitement des alertes peuvent être identifiés :

- *traitement par des équipes spécialisées :* l'analyse des alertes est effectuée par des équipes dédiées, au sein d'équipes conformité ou sécurité financière. Ces équipes peuvent être étendues à la région EMEA, en particulier dans le cadre de groupes importants au niveau européen ou mondial mais dont la présence en France est plus limitée ;
- *traitement en entonnoir :* le premier niveau de traitement est assuré par les opérationnels, puis l'alerte est escaladée à la conformité pour une analyse en deuxième niveau, complétée pour certaines entités par un troisième niveau de traitement ;
- *traitement en entonnoir inversé :* analyse en premier niveau par les équipes conformité et renvoi en deuxième niveau aux spécialistes métiers.

## 5.2. Définition d'indicateurs de priorité

Une majorité d'établissements indique que leur outil de surveillance automatisée des opérations définit un niveau de priorité de l'alerte. Les critères de priorisation incluent les facteurs suivants :

- s*coring* de l'alerte issu de l'outil, qui peut être combiné avec la notation du client ;
- type d'alerte (si, par exemple, elle est issue d'un scénario relevant du financement du terrorisme) ;
- ancienneté de l'alerte ;
- pays impliqués dans la transaction.

Pour les grands groupes, l'existence ou la forme des indicateurs de priorité varient en fonction des lignes métiers.

Un groupe a recours au *machine learning* pour hiérarchiser les alertes générées, en les classant selon leur probabilité d'aboutir à une DS. À noter que cette approche peut être mise en regard avec celle d'un autre groupe qui utilise également le *machine learning* pour déterminer une probabilité d'escalade, mais la met à profit pour ne pas générer l'alerte afin de rationaliser le flux d'alertes confiées pour investigation aux analystes (étant précisé que les alertes éliminées font l'objet d'une analyse manuelle régulière pour éviter de pérenniser un biais).

## 5.3. Éléments d'aide à la décision

La moitié des participants indique disposer d'éléments d'aide à la décision qui prennent des formes variables. Une large part d'entre eux précise que les outils automatisés de surveillance des opérations intègrent un historique des alertes relatives au client ainsi que des informations concernant le type d'alerte déclenchée (caractéristiques des scénarios notamment).

Quelques pratiques plus avancées peuvent être relevées :

- outil d'analyse des flux du client visé par l'alerte sur 13 mois voire outil d'analyse graphique permettant des analyses de réseau ;
- accès à des données plus précises sur le client directement dans l'outil de traitement des alertes (adresses IP de connexion, documents/contrats archivés du dossier client) ;
- outil d'analyse des alertes présentes dans l'historique.

### 5.4. Externalisation du traitement des alertes

Les réponses ne mentionnent pas d'externalisation extra-groupe en matière de traitement des alertes LCB-FT. En revanche, les approches d'externalisation intra-groupe sont fréquentes.

Concernant les succursales d'organismes de l'EEE, il est constaté une forte tendance à la centralisation du dispositif de traitement des alertes au niveau de l'échelon européen du groupe. Ce traitement est largement externalisé à des structures spécialisées du groupe (situées hors de France), en matière de traitement des alertes sur la zone EMEA, une faible part des alertes remontant in fine jusqu'à l'entité française. L'implication limitée des succursales dans le dispositif de traitement des alertes peut induire une maîtrise amoindrie du risque (cf. infra). Ce facteur de risque est susceptible d'être renforcé par une information insuffisante concernant les contrôles exercés sur les structures chargées du traitement des alertes. Pour les entités dont les sièges sont hors de l'EEE, une moindre tendance à l'externalisation du traitement des alertes hors de France est constatée.

Les grands groupes français disposant d'entités spécialisées par lignes métiers et/ou zone géographique ont également développé des approches d'externalisation intra-groupe du traitement des alertes. Ainsi, il est observé la plupart du temps une centralisation du traitement, leurs filiales ou succursales ne traitant pas les alertes. Dans le cas d'une organisation reposant sur le traitement des alertes par une ou des unités *offshore* en premier niveau, les deuxième et troisième niveaux de traitement, à savoir respectivement celui des examens renforcés et des déclarations de soupçon, sont, le plus souvent, du ressort d'unités *onshore*.

La centralisation du traitement des alertes peut apporter des avantages :

- une plus grande spécialisation des équipes en charge de l'analyse, qui peuvent développer une expertise plus pointue sur certaines typologies ou sur certaines géographies ;
- une meilleure gestion des pics d'activités, des absences imprévues et d'éventuels dysfonctionnements de l'outil ;
- une vision globale du client, lorsqu'une même personne peut être cliente de plusieurs entités (par exemple des comptes dans une filiale bancaire, des crédits à la consommation ou du leasing, de l'assurance vie ou des produits financiers dans des filiales spécialisées, ou encore des entreprises internationales ayant des relations avec des entités dans plusieurs pays).

Néanmoins, la centralisation expose à plusieurs risques :

- une mauvaise connaissance de la langue et donc une moindre capacité à comprendre les mentions sur les relevés de comptes, les virements, les justificatifs du client, lorsque les analystes ne sont pas francophones ;
- une moindre connaissance de la France et de ses risques : par exemple, une méconnaissance des différents types d'aides publiques ou d'aides sociales, des organismes susceptibles de les payer, et les conditions associées à ces aides, rendront l'analyste moins à même de repérer le blanchiment d'une fraude aux aides sociales. Il en est de même pour les règles fiscales, les marchés publics, les règles relatives aux plafonnements des paiements en espèces, les différents types de jeux et leur réglementation, le droit et le fonctionnement des associations,

etc. Plus généralement, un analyste éloigné de la clientèle aura une moindre capacité à repérer la proximité ou au contraire l'éloignement géographique de contreparties, ou à détecter des anomalies concernant l'implantation d'un client.

Certains participants ont indiqué que l'importance de la localisation variait selon la ligne métier : par exemple, la localisation paraissait importer moins pour la vigilance portant sur des opérations de clients qui sont des groupes internationaux. Certains ont également relevé que, quelle que soit la localisation, la formation des analystes et le contrôle de la qualité des analyses permettaient de réduire les risques associés à la configuration des modalités de traitement des alertes.

### 5.5. Suivi du délai de traitement des alertes

Des délais de traitement des alertes sont définis pour une part notable des participants. Il arrive que les procédures internes précisent un délai maximal de traitement. Toutefois, ceux-ci peuvent être particulièrement longs, allant jusqu'à 95 jours.

Un seul participant mentionne l'existence de seuils de déclenchement d'un plan de remédiation en cas d'augmentation du stock d'alertes non traitées. Peu de participants disposent d'un plan préalablement défini prévoyant des actions à mettre en œuvre en cas d'augmentation du stock d'alertes non traitées.

Un organisme d'assurance se distingue par l'absence de suivi du délai de traitement des alertes, celles-ci apparaissant uniquement en « pop-up » dans l'outil de gestion en amont de la validation de l'opération.

## 6. PLAN D'URGENCE ET DE POURSUITE DE L'ACTIVITÉ

### 6.1. Nature des mécanismes de secours

Si la grande majorité des participants a prévu des mécanismes de secours en cas d'indisponibilité du ou des outils de surveillance à travers un voire parfois plusieurs serveurs/sites d'hébergement et/ou serveurs/sites de repli, ce n'est pas le cas de tous. Quelques-uns semblent considérer le travail à distance en cas d'indisponibilité d'accès au site comme un mécanisme de secours, sans effet selon eux sur l'accès à l'outil (ce qui ne répond pas à l'hypothèse de l'indisponibilité momentanée de l'outil). Un participant a indiqué que son outil de surveillance étant indissociable du fonctionnement de son système de *core banking*, il n'avait mis à ce stade aucun mécanisme de secours, un arrêt de ce système étant synonyme d'arrêt des flux. Un établissement de taille modeste a également signifié qu'il était actuellement en train de déterminer sa politique et ses procédures en matière de mécanismes de secours en cas d'indisponibilité des outils de surveillance automatisée des opérations.

Dans le but de se prémunir de tout dysfonctionnement susceptible d'entraîner un arrêt de la génération ou du traitement des alertes, certains participants ont mis en place des dispositifs de contrôle dédiés tels que :

- un suivi du statut des processus prévoyant l'envoi d'un courriel quotidien de notification au responsable de la conformité attestant du bon fonctionnement de l'outil ;
- des sauvegardes et des copies instantanées en cas de dysfonctionnement et d'indisponibilité des serveurs, afin de garantir une reprise du stock d'alertes existants ;
- une rotation semestrielle des centres de données utilisées.

## 6.2. Test des mécanismes de secours

La plupart des participants ont défini des plans de secours, lesquels sont testés généralement une fois par an. Pour certains d'entre eux, ils ont été définis au niveau du groupe et la conduite de tests est également réalisée à ce niveau. Par ailleurs, la crise sanitaire récente a constitué un test partiel des dispositifs de traitement des alertes, sous la contrainte d'un accès distant à ces dispositifs.

Aucune défaillance majeure nécessitant la mise en œuvre opérationnelle de mécanismes de secours n'a été identifiée ces dernières années par les participants, si ce n'est une attaque virale dans un organisme ayant occasionné un arrêt momentané de l'outil de surveillance. Cet organisme a indiqué avoir été en mesure de récupérer puis de traiter correctement l'ensemble des alertes passées et apparues pendant le temps de l'arrêt.

## 6.3. Définition des indicateurs de résilience

Certains participants ont défini des indicateurs de période d'indisponibilité maximale tolérée de l'outil, plus particulièrement ceux ayant fait le choix de recourir à l'externalisation en matière d'outil de surveillance automatisée des opérations. Dans ce cas, la durée maximale pour le rétablissement du service est le plus fréquemment de 24 heures, en particulier pour les prestataires de services de paiement. Dans quelques cas, la durée était plus longue: un cas à 7 jours, un autre à 10 jours et un à 15 jours.

Si la grande majorité des participants signalent être en mesure de rattraper l'intégralité des opérations a posteriori en cas de dysfonctionnement momentané, ce n'est pas le cas de tous.