Groupe d'action financière sur le blanchiment de capitaux

Financial Action Task Force on Money Laundering

Rapport sur les typologies du blanchiment de capitaux et du financement du terrorisme 2003-2004

Secrétariat du GAFI
2, rue André-Pascal
75775 Paris Cedex 16
FRANCE

Contact@fatf-gafi.org

TABLE DES MATIÈRES

SYNTHÈSE **1**

INTRODUCTION **3**

I. LES VIREMENTS ÉLECTRONIQUES ET LEUR RÔLE DANS LE FINANCEMENT DU TERRORISME **5**

Typologies 6
Conséquences au plan de l'action publique 8

II. LES ORGANISMES À BUT NON LUCRATIF ET LEUR RÔLE DANS LE FINANCEMENT DU TERRORISME **10**

Typologies 10
Conséquences au plan de l'action publique 15

III. LES RISQUES DE BLANCHIMENT DANS LE SECTEUR DE L'ASSURANCE **18**

Typologies 18
Conséquences au plan de l'action publique 21

IV. LES PERSONNES POLITIQUEMENT EXPOSÉES **23**

Conséquences au plan de l'action publique 26

V. LES OUVREURS DE PORTE (OU « GATEKEEPERS ») ET LE BLANCHIMENT DE CAPITAUX **28**

Conséquences au plan de l'action publique 31

CONCLUSION **32**

LISTE DES EXEMPLES

Exemple 1 : Fonds collectés dans un pays A et transférés à une organisation terroriste dans un pays B 6

Exemple 2 : Virements utilisés par une organisation terroriste pour transférer de l'argent afin de poursuivre ses activités au-delà des frontières 6

Exemple 3 : Utilisation de virements dans le cadre d'une campagne de collecte de fonds terroristes 7

Exemple 4 : Fractionnement des paiements de manière à éviter toute détection 7

Exemple 5 : Collecte de fonds par l'intermédiaire d'un OBNL 11

Exemple 6 : Utilisation d'un OBNL pour transférer de l'argent à des personnes soupçonnées de terrorisme 11

Exemple 7 : Utilisation d'OBNL pour procéder à des transferts illégaux 12

Exemple 8 : Utilisation d'un OBNL par des membres de sa direction pour financer le terrorisme 12

Exemple 9 : Utilisation d'une police d'assurance pour blanchir de l'argent 19

Exemple 10 : Blanchiment de sommes versées par une compagnie d'assurance 19

Exemple 11 : Utilisation de l'assurance pour blanchir des capitaux 20

Exemple 12 : Des membres d'un réseau de criminalité organisée blanchissent de l'argent grâce à des polices d'assurance-vie 21

Exemple 13 : Blanchiment d'argent obtenu dans le cadre d'une opération de corruption à grande échelle par un proche d'une PPE 23

Exemple 14 : Un haut fonctionnaire de l'État blanchit de l'argent obtenu par détournement de fonds publics grâce à des membres de sa famille 24

Exemple 15 : Implication d'un cadre d'une entreprise publique dans une opération de corruption à haut niveau 25

Exemple 16 : Blanchiment des produits de détournements de fonds 26

Exemple 17 : Un comptable et des avocats prêtent la main à une opération de blanchiment 28

Exemple 18 : Des juristes professionnels participent à une opération de blanchiment 29

Exemple 19 : Un comptable prodigue des conseils financiers spécialisés à des représentants de la criminalité organisée 29

Exemple 20 : Un avocat utilise des sociétés extraterritoriales et des comptes en fiducie pour blanchir des capitaux 29

Exemple 2 1: Un avocat utilise le compte d'un client pour faciliter une opération de blanchiment 30

Exemple 22 : Utilisation d'un fonds en fiducie pour recevoir de l'argent sale et acquérir des biens immobiliers 30

SYNTHÈSE

1. La participation des membres du GAFI, de plusieurs non membres du GAFI et d'organisations internationales à l'exercice sur les typologies 2003-2004 a permis de donner une perspective internationale aux tendances actuelles du blanchiment de capitaux et du financement du terrorisme. Cette année, les thèmes abordés ont été les suivants : les virements électroniques et les organismes à but non lucratif (OBNL) et leurs liens avec le financement du terrorisme, la vulnérabilité du secteur des assurances au regard du blanchiment de capitaux, les personnes politiquement exposées (PPE) et les « ouvreurs de portes » ou « gatekeepers ».

2. Les virements électroniques constituent un moyen rapide et efficace de déplacer des fonds, et ils peuvent de ce fait être utilisés à des fins terroristes. Il est ainsi possible de mettre en place des schémas complexes de virements électroniques à la seule fin de brouiller délibérément le suivi de la transaction et de dissimuler l'origine et la destination des fonds destinés à un usage terroriste. À l'heure actuelle, un nombre limité d'indicateurs permettant de repérer des virements électroniques potentiellement de nature terroriste est disponible : il s'agit essentiellement de l'origine et de la destination des fonds, ainsi que de l'identité des personnes participant à la transaction, pour autant que cette information soit disponible. Les participants à l'exercice annuel 2003-2004 ont admis la nécessité d'élaborer d'autres indicateurs permettant de définir des opérations potentiellement suspectes.

3. L'examen de l'utilisation abusive d'organismes à but non lucratif à des fins terroristes a montré que le détournement d'un volume de fonds même très faible pouvait dissimuler un problème de financement d'activités terroristes potentiellement grave. Différentes catégories d'organismes à but non lucratif ont été recensées, et pour chaque catégorie, une série de profils de risque a été ébauchée. Même si dans la plupart des pays, les pouvoirs publics arrivent dans une certaine mesure à réglementer et à surveiller le secteur à but non lucratif, des mesures additionnelles sont probablement nécessaires afin de réduire l'utilisation abusive de ces organismes. Les experts ont conclu que le besoin existe de développer et de renforcer les mécanismes et canaux d'échange de renseignements afin de contrer le risque de financement du terrorisme.

4. L'exercice a par ailleurs permis de confirmer que le secteur des assurances présentait un certain nombre de vulnérabilités en termes de blanchiment de capitaux. De fait, le manque de cohérence de la réglementation de cette activité est un point faible qui pourrait être exploité par les blanchisseurs. D'une manière générale, la vulnérabilité la plus grande de ce secteur se situe lors de la phase d'intégration du cycle du blanchiment de capitaux. On a pu constater que le volume de blanchiment détecté était faible comparé à la taille du secteur dans son ensemble. Il est probable que cette constatation demandera à être approfondie afin de parvenir à une meilleure compréhension des risques spécifiques de blanchiment de capitaux dans chacun des différents secteurs qui composent cette branche d'activité.

5. Les personnes politiquement exposées (PPE) sont des personnes qui exercent, ou qui ont par le passé exercé des fonctions publiques de premier plan dans un pays donné. La presse fait souvent état de révélations selon lesquelles des PPE sont soupçonnées d'activité criminelle de nature financière, en particulier de corruption. Les PPE, lorsqu'elles sont impliquées dans des activités criminelles, dissimulent souvent les biens qu'elles ont obtenus de manière illicite dans un réseau d'entités fictives ou de banques offshore situées dans un autre pays que leur pays d'origine. On a constaté qu'elles avaient souvent recours à des intermédiaires ou à des membres de leur famille pour transporter ou détenir des biens pour leur propre compte. Les techniques utilisées par les PPE pour dissimuler leurs biens sont les mêmes que celles mises en œuvre par les blanchisseurs d'argent. Les institutions financières peuvent donc arriver à détecter leurs activités illégales éventuelles en appliquant des mesures de vigilance accrues semblables à celles applicables dans le cadre de la lutte contre le blanchiment de capitaux.

6. Enfin, il arrive de plus en plus fréquemment que les blanchisseurs cherchent à obtenir des conseils ou à s'adjoindre les services de professionnels spécialisés afin de faciliter leurs opérations

financières. Cette tendance à l'implication de différents experts juridiques et financiers, ou « ouvreurs de portes », dans les opérations de blanchiment a déjà été constatée par le GAFI, et il semble qu'elle se poursuive. Les travaux menés dans le cadre de l'exercice de cette année ont confirmé et approfondi ce que le GAFI savait déjà des caractéristiques propres à ce secteur, et ce qui le rend vulnérable au blanchiment. Une des importantes conclusions à laquelle sont parvenus les experts consultés est qu'un grand nombre des risques associés aux « ouvreurs de portes » pourraient être réduits si les mesures de lutte contre le blanchiment et le financement du terrorisme étaient appliquées d'une manière complète et cohérente.

INTRODUCTION

7. Le blanchiment de capitaux et le financement du terrorisme sont deux types de criminalité financière dont les effets dévastateurs vont bien au-delà d'opérations financières apparemment inoffensives. Qu'il s'agisse des profits réalisés par des trafiquants de drogue de petite envergure ou du détournement des deniers de l'État par des fonctionnaires indélicats, les produits d'activités criminelles ont le pouvoir de corrompre et, en dernier ressort, de déstabiliser des communautés, voire des économies nationales dans leur ensemble. Les réseaux terroristes sont à même d'exercer leurs activités insidieuses, à l'échelle mondiale et dans les lieux que l'on avait cru jusqu'alors épargnés par ce phénomène, en s'appuyant sur des structures financières non décelées. Que l'on ait affaire à des criminels ou à des terroristes, tous sont capables d'exploiter les lacunes ou autres points faibles du système financier légitime pour blanchir les produits de leurs activités criminelles ou soutenir leurs activités terroristes.

8. Le Groupe d'action financière (GAFI) procède chaque année à un examen des méthodes et des tendances (« typologies ») du blanchiment de capitaux et, depuis 2001, du financement du terrorisme. L'un des principaux objectifs de ce travail consiste à recueillir des éléments qui aideront les responsables de l'action publique dans les pays membres du GAFI à élaborer et à affiner les normes de lutte contre le blanchiment et le financement du terrorisme. En outre, les conclusions obtenues à l'issue de cet exercice annuel permettent d'informer un public plus large (autorités de réglementation, instances opérationnelles et cellules de renseignements financiers et grand public) des caractéristiques et tendances du blanchiment des capitaux et du financement du terrorisme.

9. L'exercice annuel du GAFI sur les typologies trouve son point d'orgue dans une réunion d'experts. Celle de cette année s'est tenue les 17 et 18 novembre 2003 à Oaxaca, au Mexique, sous la présidence de Madame María de la Concepción Patiño Cestafe, Chef de la *Dirección General Adjunta de Investigación de Operaciones (DGAIO)*, cellule mexicaine de renseignements financiers. Trente-cinq pays et territoires, parmi lesquels les représentants des pays membres du GAFI, ont participé à cette réunion : Afrique du sud ; Allemagne ; Argentine ; Australie ; Autriche ; Belgique ; Brésil ; Canada ; Conseil de coopération du Golfe; Danemark ; Espagne ; Etats-Unis ; France ; Hong Kong, Chine ; Italie ; Japon ; Luxembourg ; Mexique ;; Norvège ; Nouvelle-Zélande ; Pays-Bas ; Portugal ; Royaume-Uni ; Singapour ; , Suède et Suisse. Ont également participé à cette réunion des représentants des organismes régionaux de type GAFI : le Groupe Asie/Pacifique sur le blanchiment de capitaux (GAP, avec des représentants de la Corée, de l'Inde et le Secrétariat de l'AGP), le Groupe d'action financière des Caraïbes (GAFIC, avec des représentants des Bahamas, du Salvador, du Guatemala, du Honduras, de Panama et du Venezuela), le Groupe d'action financière sur le blanchiment de capitaux en Amérique du sud (GAFISUD) et le Comité d'experts du Conseil de l'Europe sur l'évaluation des mesures anti-blanchiment (MONEYVAL, avec des représentants de Monaco, de la Roumanie et de l'Ukraine). Les organisations suivantes avaient par ailleurs envoyé des représentants : le Groupe Egmont des cellules de renseignements financiers, Europol, le Fonds monétaire internationale (FMI), l'Association Internationale des services de Contrôle des Assurances (AICA ou *International Association of Insurance Supervisors, IAIS*), l'Organisation internationale des commissions de valeurs (OICV), Interpol, le Groupe des organismes de supervision offshore (GOSBO), l'Organisation des États américains (OEA) et la Banque mondiale.

10. Chaque année, l'analyse des typologies réalisée par le GAFI met l'accent sur une série de points ou de thèmes sélectionnés lors de la réunion plénière du GAFI. Les participants à la réunion plénière s'efforcent de choisir ces thèmes en fonction des travaux en cours au sein du GAFI, ou bien des suites à donner à des méthodes ou tendances identifiées lors d'exercices précédents. Cinq thèmes ont ainsi été retenus cette année. L'examen des liens entre le financement du terrorisme et les virements électroniques d'une part et les organismes à but non lucratif (OBNL) d'autre part sont deux des thèmes ainsi sélectionnés pour l'exercice du GAFI-XV. Ils s'inscrivent dans le cadre de travaux antérieurs sur les typologies, et pourront être utilisés pour affiner les lignes directrices publiées par le GAFI dans le cadre des Huit Recommandations Spéciales sur le financement du terrorisme. Le troisième thème, la vulnérabilité du secteur des assurances au regard du blanchiment de capitaux, a été choisi afin de

revenir, en les approfondissant, sur des conclusions initiales tirées de travaux antérieurs du GAFI sur les typologies. Enfin, le GAFI s'est penché sur les risques de blanchiment associés aux personnes politiquement exposées (PPE) et aux prestataires de services financiers spécialisés, les « ouvreurs de porte ». Depuis la publication de la version révisée des Quarante Recommandations du GAFI en juin 2003, des mesures s'appliquent aux PPE et aux « ouvreurs de porte », c'est pourquoi l'examen des typologies de cette année visait à recueillir des informations complémentaires sur la nature et sur l'ampleur de la menace propre à ces deux domaines.

11. Le format retenu pour la réunion d'experts chargés de mener à bien l'exercice sur les typologies du GAFI-XV a été légèrement différent de celui qui était en vigueur les années précédentes. Pour trois des thèmes en effet, à savoir les virements électroniques, les organismes à but non lucratif et la vulnérabilité du secteur des assurances, un certain nombre de travaux ont été effectués en petits comités avant la réunion des experts, de manière à bien centrer les discussions sur les thèmes retenus. Ensuite, au cours de la réunion même, chacun de ces thèmes a fait l'objet d'une session séparée plus restreinte (à laquelle ont participé une trentaine de membres des autorités opérationnelles et des organes de décision) dans le but de dégager les grandes tendances et d'examiner les implications, en termes d'action publique, de l'examen des typologies recensées. Les conclusions de ces trois ateliers ont été ensuite soumises à l'ensemble des participants et ont donc pu être à nouveau débattues parallèlement à la présentation des sujets consacrés aux PPE et aux « ouvreurs de portes ».

12. Ce rapport du GAFI-XV sur les typologies du blanchiment expose les principales conclusions tirées à l'issue de l'examen de chacun des thèmes telles qu'elles ressortent des trois ateliers, de la réunion de l'ensemble des experts et des contributions écrites soumises par les délégations participantes avant la réunion. Comme c'est l'usage au GAFI, le rapport présente des études de cas tirées des contributions écrites et des interventions faites pendant la réunion. Les textes de ces exemples sont reproduits ci-après, dans la mesure du possible, tels qu'ils ont été soumis dans l'optique de cet exercice. Toutefois, les noms des pays ont été modifiés, de même que les devises et certains autres éléments, de manière à préserver certains aspects sensibles des affaires citées à cette occasion.

I. LES VIREMENTS ÉLECTRONIQUES ET LEUR RÔLE DANS LE FINANCEMENT DU TERRORISME

13. Les terroristes ont recours aux virements électroniques pour transférer les fonds nécessaires au financement de leurs activités. La structure d'assise financière mise à jour après les attaques du 11 septembre aux Etats-Unis a montré le rôle essentiel joué par les virements électroniques pour procurer aux pirates de l'air les moyens financiers dont ils avaient besoin pour préparer et ensuite mener à bien leurs attaques.[1] C'est cette utilisation des virements électroniques que le GAFI avait en tête lorsqu'il a publié en octobre 2001 sa Recommandation Spéciale VII. Afin de regrouper toutes les informations dont on dispose sur les caractéristiques et le rôle des virements électroniques dans le financement du terrorisme, le GAFI a choisi de consacrer à cette question le premier des ateliers organisés au cours de sa réunion annuelle sur les typologies.

14. Les expressions « virement électronique » et « virement de fonds » utilisées par le GAFI désignent toute transaction financière effectuée par voie électronique au nom d'un donneur d'ordre via une institution financière en vue de mettre à disposition d'un bénéficiaire une certaine somme d'argent dans une autre institution financière. Dans certains cas, le donneur d'ordre et le bénéficiaire peuvent être une seule et même personne.[2] Les virements électroniques peuvent être nationaux ou internationaux. Étant donné qu'ils n'entraînent aucun mouvement physique de devises, ils constituent un moyen rapide et sûr pour transférer des fonds d'un lieu à un autre.

15. Aujourd'hui, les systèmes de paiement, aussi bien pour les opérations interbancaires que pour la banque de détail, assurent une meilleure couverture et une plus grande efficacité des virements électroniques nationaux et internationaux. Le développement continu de réseaux mondiaux tels que SWIFT a accru la fiabilité et l'efficacité des systèmes de paiement interbancaires, si bien qu'un grand nombre de transactions peuvent être traitées quotidiennement. Dans le secteur de la banque de détail, des services tels que les services bancaires par téléphone et sur l'Internet permettent aux clients d'effectuer des transactions à distance, à partir de n'importe quel lieu dûment équipé.

16. Les progrès accomplis en matière de technologie des systèmes de paiement ont eu un double impact du point de vue du détournement potentiel de ces systèmes par ceux qui financent le terrorisme et ceux qui blanchissent l'argent sale. D'un côté, les systèmes de paiement électroniques offrent une plus grande sécurité parce qu'il est plus facile de suivre la trace des différentes transactions grâce à des registres électroniques qui peuvent être automatiquement générés, tenus et/ou transmis en même temps que la transaction elle-même. De l'autre côté en revanche, ces progrès sont également sources de caractéristiques susceptibles d'attirer les terroristes ou blanchisseurs en puissance. Par exemple, l'augmentation de la vitesse et du volume des virements, conjuguée à l'absence de cohérence dans les méthodes permettant d'enregistrer des informations essentielles sur ces transactions, d'en garder la trace et de transmettre les informations nécessaires en même temps que les transactions, sont un obstacle à la traçabilité des transactions individuelles pour les autorités chargées d'enquêter sur elles.

17. Une autre complication existe sous la forme des transferts effectués par l'entremise d'institutions financières non bancaires telles que les services de remise de fonds, bureaux de change et autres activités similaires. Dans certains pays, ces bureaux procèdent à des virements électroniques, soit directement dans des bureaux correspondants, dans le même pays ou à l'étranger, soit par le biais d'institutions financières traditionnelles (comme les banques par exemple). Là encore, les différences qui existent entre les obligations en matière d'enregistrement ou de transmission d'informations sur le

[1] Voir la déclaration du « Federal Bureau of Investigation » devant le Congrès des Etats-Unis, qui était citée dans le rapport du GAFI de l'année dernière et qui peut être consultée sur le site http://www.fbi.gov/congress/congress02/lormel021202.htm. Cette déclaration décrit les profils financiers des pirates de l'air du 11 septembre et mentionne le recours à des virements électroniques pour le transfert de fonds.

[2] Voir la Note interprétative à la Recommandation Spéciale VII : Virements électroniques.

donneur d'ordre à l'origine des transferts ainsi effectués peuvent être mises à profit par les terroristes ou d'autres criminels désireux de transférer des fonds sans qu'il soit facile aux autorités de les repérer.

Typologies

18. Les experts du GAFI admettent que les virements électroniques constituent un moyen rapide et efficace pour transférer des fonds destinés à des fins terroristes. Par exemple, un réseau simple de transmission de fonds terroristes peut être mis sur pied simplement en exploitant les différences qui existent entre les régimes de contrôle en vigueur dans différents pays. De fait, si aucun dossier relatif au donneur d'ordre n'est constitué au point de départ du virement, ou si les informations cessent d'être relayées par un intermédiaire à un point quelconque de la chaîne, les enquêteurs ne pourront pas avoir accès aux renseignements qui pourraient les aider à établir l'existence de liens avec le terrorisme.

19. On a pu observer des montages encore plus compliqués, mettant en jeu une multiplicité de virements électroniques qui ont pour effet de créer un ensemble de transactions financières complexe et délibérément obscur dans le but d'éviter tout repérage.

20. Un certain nombre de caractéristiques communes ont été également relevées comme méritant d'être citées dans les typologies du financement potentiel du terrorisme au moyen de virements électroniques. L'une d'entre elles, importante, est le recours à de fausses identités, à des « hommes de paille » ou à des sociétés-écrans afin de fournir des noms irréprochables et d'éviter tout repérage. Une autre caractéristique consiste à faire transiter les fonds par plusieurs institutions financières différentes afin que les virements aient l'air de venir de sources multiples et apparemment sans lien entre elles. Il semble par ailleurs que des terroristes effectuent quelquefois des virements par l'intermédiaire d'institutions financières non bancaires ou de services alternatifs de remise de fonds (systèmes informels de transfert de fonds ou de valeurs) dans l'idée qu'en évitant les grandes institutions financières officielles, il sera plus facile de rendre le financement du terrorisme (de même que les produits d'activités criminelles non terroristes) indécelable par les systèmes de surveillance financière et les autorités chargées d'effectuer des enquêtes.

Exemple 1 : Fonds collectés dans un pays A et transférés à une organisation terroriste dans un pays B

Une organisation terroriste utilisait ses contacts à l'étranger pour « taxer » une communauté d'expatriés sur leurs revenus et leur épargne. Les montants ainsi prélevés étaient déposés sur un fonds et transmis ensuite par virements électroniques à un bureau de représentation, qui constituait également l'aile politique du groupe basé dans le pays voisin.

Une importante communauté circulait entre ce pays voisin et le « pays-cible », si bien que des armes et du matériel pouvaient être achetés et passés en contrebande par la frontière à destination de la province autonome où l'organisation terroriste menait ses attaques.

Exemple 2 : Virements utilisés par une organisation terroriste pour transférer de l'argent afin de poursuivre ses activités au-delà des frontières

On s'est aperçu qu'une organisation terroriste implantée dans un pays X avait recours à des virements électroniques pour faire parvenir dans un pays Y de l'argent qui était utilisé pour payer le loyer de logements sûrs, acheter et vendre des véhicules, et acquérir des composants électroniques permettant de construire des engins explosifs. L'organisation utilisait des comptes-relais ou des comptes de transit dans le pays X pour transférer les fonds d'un pays à l'autre. Aux deux bouts de la chaîne, les comptes étaient ouverts au nom de personnes n'ayant apparemment aucun rapport avec la structure de l'association terroriste, mais ayant entre eux des liens de parenté ou autres, si bien que ces liens familiaux apparents pouvaient si nécessaire servir de justification aux transferts.

Les fonds étaient déposés sur des comptes bancaires à partir desquels les virements étaient réalisés, essentiellement sous la forme de dépôts en espèces effectués par l'organisation terroriste. Une fois l'argent

parvenu à destination, le titulaire pouvait soit le laisser sur le compte, soit l'investir dans des fonds de placement où il restait dissimulé mais disponible pour les besoins futurs de l'organisation. Sinon, l'argent pouvait aussi être transféré sur d'autres comptes bancaires gérés par le correspondant de l'organisation chargé de la gestion financière, où ils étaient utilisés pour régler l'achat de matériels et d'équipements ou pour couvrir d'autres dépenses ad hoc effectuées par l'organisation dans le cadre de ses activités clandestines.

Exemple 3 : Utilisation de virements dans le cadre d'une campagne de collecte de fonds terroristes

Une enquête menée dans un pays A sur une entreprise Z, soupçonnée de faire circuler en contrebande et de distribuer de la pseudo-éphédrine (dont on pense qu'elle constitue une source de profits pour des organisations terroristes) a montré que les salariés de l'entreprise Z envoyaient un grand nombre de chèques négociables dans le pays B. D'autres éléments ont permis de prouver que l'entreprise destinataire rendait des services de remise de fonds sans y être autorisée. Sur la base de ces informations, un mandat de perquisition a été obtenu pour les locaux de l'entreprise Z et deux résidences. L'analyse des documents et relevés bancaires saisis à l'occasion de la perquisition a montré que les suspects avaient viré électroniquement des fonds à une personne soupçonnée d'entretenir des liens avec un groupe terroriste.

Un peu plus tard la même année, les enquêteurs ont lancé une série de recherches coordonnées. Trois personnes ont été arrêtées et accusées d'avoir failli à l'obligation d'enregistrement en qualité d'entreprise financière, et environ USD 60 000 en espèces et en chèques ont été saisis. En outre, les enquêteurs ont mis à jour l'existence d'un compte bancaire contenant quelque USD 130 000 qui était utilisés pour faciliter des virements électroniques illégaux vers des destinations extérieures au pays A. Les personnes concernées n'ont pas encore été jugées.

21. Les experts assistant à la réunion de cette année sont tombés d'accord sur le fait que mis à part la taille généralement modeste de ces transactions, la valeur des virements individuels n'était généralement pas un critère permettant d'établir un objectif de financement du terrorisme. De fait, le montant modeste des virements par rapport au volume global élevé de ces transactions rend plus difficile encore le repérage de l'utilisation du système financier à des fins terroristes. Il s'est même révélé impossible d'établir une taille moyenne pour les virements électroniques effectués en liaison avec le terrorisme, bien qu'une délégation ait indiqué avoir relevé des transfert de montants situés dans une fourchette aussi faible que USD 25 à USD 500. Quelques experts ont toutefois noté que les virements semblent souvent structurés en montants inférieurs à tout seuil de déclaration obligatoire.

Exemple 4 : Fractionnement des paiements de manière à éviter toute détection

Pendant quatre ans, M. A et son oncle ont exercé des activités de remise de fonds sous la raison sociale d'une entreprise S et agi en qualité d'agents d'une plus grande société de remise de fonds soupçonnée d'être utilisée à des fins de financement du terrorisme. Une enquête a ensuite été ouverte sur l'entreprise S à la suite d'une déclaration d'opération suspecte.

L'enquête a montré que sur cette période de quatre ans, l'entreprise de M. A avait reçu plus de USD 4 million en espèces de personnes souhaitant transférer de l'argent dans différents pays. Lorsque les clients remettaient les espèces à M. A, elles étaient déposées sur de multiples comptes ouverts auprès de différentes succursales de banques dans le pays X. Afin de se soustraire aux obligations de déclaration en vigueur dans le pays X, M. A et les autres personnes impliquées déposaient toujours des sommes inférieures à USD 10 000, effectuant quelquefois de multiples dépôts de moins de USD 10 000 en une seule journée.

M. A. a été poursuivi pour association de malfaiteurs en vue de « structurer » (soit fractionner) des transactions monétaires de manière à échapper aux obligations de déclaration d'opérations financières. Il a plaidé coupable.

22. En dépit de ces quelques observations formulées à propos des virements effectués à des fins de financement du terrorisme, les experts ont réaffirmé que pour l'instant, les enquêteurs et les institutions financières ne disposaient toujours que d'un nombre limité d'indicateurs permettant de

détecter une utilisation possible des virements à des fins terroristes. Dans les cas où l'on dispose d'informations sur un virement transfrontalier particulier, les seuls facteurs qui peuvent aider à relier la transaction au financement du terrorisme sont souvent le nom du donneur d'ordre et celui du bénéficiaire, ou bien encore le lieu de destination. La taille de la transaction semble ne suivre aucun modèle spécifique, même si les experts estiment que les montants sont généralement modestes, soit parce que les opérations individuelles de financement du terrorisme ne portent pas sur de grosses sommes, soit à cause d'une volonté délibérée de fractionner les transactions pour éviter tout repérage.

Conséquences au plan de l'action publique

23. La Recommandation Spéciale VII du GAFI, ainsi que sa Note interprétative publiée ultérieurement, contiennent des lignes directrices permettant de prévenir et de détecter le recours aux systèmes de virements électroniques par des terroristes, ou par d'autres criminels n'ayant pas de lien avec le terrorisme. Cette Recommandation appelle à enregistrer, à conserver et, dans le cas de virements transfrontaliers, à transmettre certains renseignements-clés sur le donneur d'ordre. Ces renseignements, une fois parvenus à l'endroit de destination du virement, permettront aux institutions financières concernées de procéder à une évaluation initiale des liens potentiels avec les milieux terroristes/criminels (aux fins par exemple de l'établissement des déclarations d'opérations suspectes) et seront en dernière instance transmis aux cellules de renseignements financiers, autorités opérationnelles et autres autorités compétentes (aux premiers stades de leurs procédures d'analyse ou d'enquête).

24. L'ajout et la conservation de renseignements significatifs sur les donneurs d'ordres de virement peuvent contribuer à la lutte contre le financement du terrorisme et le blanchiment de capitaux de plusieurs manières. En effet, les transactions pour lesquelles les informations sont complètes aident les institutions financières bénéficiaires à identifier les opérations potentiellement suspectes. Ceci suppose de leur part la mise en œuvre de contrôles supplémentaires et la transmission potentielle des informations ainsi recueillies à une cellule de renseignements financiers. Lorsqu'une cellule de renseignements financiers reçoit des déclarations relatives à un virement inhabituel ou suspect, celles qui contiennent des renseignements exhaustifs peuvent faire l'objet de recherches et d'analyses plus complètes. Enfin, le fait de vérifier que les informations relatives aux donneurs d'ordre sont facilement accessibles aide les autorités opérationnelles concernées à repérer les terroristes et autres criminels, à enquêter sur eux et à engager les poursuites nécessaires.

25. Si l'atelier n'avait pas pour objet de se pencher sur l'efficacité ou l'opportunité globale des mesures préconisées dans la Recommandation Spéciale VII, de l'avis général des participants, ces mesures ont été jugées favorables. De fait, pouvoir mettre des renseignements « complets et utiles » sur le donneur d'un ordre de virement à la disposition des institutions financières et des autorités compétentes a été jugé essentiel pour pouvoir détecter ou empêcher l'utilisation des virements électroniques à des fins terroristes ou criminelles.

26. La note interprétative à la Recommandation Spéciale VII publiée en février 2003 autorise pour l'instant à instituer un seuil de minimis de USD 3 000 pour les mesures préconisées dans la Recommandation. Ainsi, même si les pays doivent toujours obliger les institutions à noter et à conserver des informations sur les donneurs d'ordres de virements inférieurs à ce montant, la transmission de ces renseignements en même temps que le virement n'est pas obligatoire. Les experts ont débattu pour savoir s'il fallait ou non fixer un seuil pour les mesures relatives aux virements figurant dans la Recommandation Spéciale VII. La majorité d'entre eux ont fait valoir que les transactions par virement ayant un lien potentiel avec le terrorisme portent généralement sur des montants peu élevés. Un consensus s'est dégagé sur le fait que l'existence d'un seuil pour les obligations contenues dans la Recommandation Spéciale VII pourrait, du point de vue opérationnel, faire obstacle à la détection de transactions éventuellement pertinentes. Certains participants ont également fait remarquer que l'absence de seuil, en rendant le risque de détection plus grand, pouvait dissuader les terroristes ou les criminels de recourir aux virements électroniques.

27. Cependant, les experts ont également admis qu'en l'absence d'autres indicateurs spécifiques, le fait de ne pas fixer de seuil risquait d'aboutir à ce qu'un nombre excessif d'opérations soient signalées aux cellules de renseignements financiers. Les déclarations relatives à des transactions individuelles auront peut-être moins de valeur comme moyen de détection du financement du terrorisme, mais elles sont importantes car, lorsqu'elles sont détectées par d'autres moyens (par exemple grâce à des comptes rendus ou enquêtes émanant d'autres organismes), elles permettent de se faire une idée des structures financières qui servent d'appui au terrorisme. Comme déjà indiqué, les éléments les plus important pour détecter des virements électroniques effectués en liaison avec des activités terroristes sont pour l'instant les noms des parties concernées et l'origine ou la destination géographiques de la transaction. Les experts sont en conséquence tombés d'accord sur le fait qu'il fallait poursuivre les travaux pour définir des indicateurs plus précis de l'utilisation des virements électroniques à des fins terroristes. Ces indicateurs devront aider les institutions financières à identifier les opérations qui sont susceptibles de nécessiter une surveillance accrue et qui, en dernier ressort, devront être portées à la connaissance des autorités compétentes si elles apparaissent comme suspectes ou inhabituelles.

28. Une solution potentielle pour trouver des indicateurs supplémentaires serait d'encourager la mise au point de systèmes informatiques capable de rechercher des indicateurs objectifs dans les virements électroniques. Une des délégations a proposé d'utiliser un système qui repérerait de tels indicateurs à partir de mots-clés apparaissant dans les messages accompagnant les virements. En établissant un score à partir de différentes valeurs affectées à ces mots-clés, le système pourrait sélectionner un petit groupe d'opérations nécessitant éventuellement une analyse plus approfondie.

II. LES ORGANISMES À BUT NON LUCRATIF ET LEUR RÔLE DANS LE FINANCEMENT DU TERRORISME

29. Le GAFI s'était déjà penché sur le rôle des organismes à but non lucratif (OBNL) dans le cadre de son dernier exercice sur les typologies (2002-2003). A cette époque, il avait pu formuler certaines conclusions préliminaires sur la nature des risques inhérents à ce secteur. Afin d'approfondir ces travaux, il a été décidé de revenir sur la question des OBNL et de leur détournement potentiel à des fins de financement du terrorisme, qui a fait l'objet du deuxième atelier pour l'exercice de cette année. Comme indiqué en introduction, les trois ateliers ont été précédés de travaux préparatoires avant la réunion des experts. La préparation de l'atelier sur les OBNL est celle qui a été la plus complète, avec plusieurs petites réunions d'experts et de nombreux échanges d'analyses et de notes exposant les positions des différents intervenants. C'est pour cette raison que l'atelier sur les OBNL a pu parvenir, dans ses conclusions, à un niveau de détail dont le présent rapport est le reflet.

30. Si certains pays ont une expérience relativement étendue du financement du terrorisme par le biais des OBNL, d'autres pays n'en ont à l'évidence qu'une expérience plus limitée. Seuls quelques-uns des éléments fournis dans le cadre de l'exercice de cette année concernaient des cas de financement *avéré* du terrorisme. L'essentiel des pièces concernait donc des cas de financement du terrorisme *soupçonné* ou *possible* (un grand nombre faisant d'ailleurs l'objet d'enquêtes encore en cours), tandis que quelques autres concernaient d'autres formes possibles de recours abusif à des OBNL.

31. La plupart des pays partagent les inquiétudes relatives aux difficultés rencontrées pour détecter le financement du terrorisme au moyen du détournement d'OBNL. Il est généralement admis que de tels organismes jouent un rôle d'accompagnement social et financier essentiel dans toutes les sociétés, et ce rôle n'est à l'évidence pas remis en question. Néanmoins, le simple volume des fonds et des actifs détenus par le secteur des OBNL fait que le détournement ne serait-ce que d'un infime pourcentage de ces fonds à des fins de financement du terrorisme constituerait déjà un problème grave. Ainsi, le peu d'informations disponibles sur l'ampleur avec laquelle les terroristes exploitent peut-être ce secteur doit être considérée en soi comme un sujet de préoccupation sérieux pour la communauté internationale dans son ensemble.

32. Les OBNL possèdent des caractéristiques qui les rendent particulièrement vulnérables à un détournement à des fins de financement du terrorisme. Ils jouissent en effet de la confiance du public, ont accès à des sources de financement considérables et voient souvent circuler beaucoup de liquidités. En outre, certains d'entre eux ont une implantation internationale qui sert de cadre à des activités et opérations financières nationales et internationales, souvent à l'intérieur ou à proximité des zones qui sont justement le plus exposées aux activités terroristes. Enfin, selon le pays et la forme juridique des OBNL, ils sont souvent soumis à une réglementation peu contraignante, voire inexistante (par exemple en ce qui concerne les obligations d'enregistrement, de comptabilité, d'information financière et de contrôle), ou bien alors leur création est relativement facile (par exemple aucune compétence ou aucun capital de départ n'est requis, il n'est pas nécessaire de vérifier les antécédents des employés, etc.).

Typologies

33. Les études de cas exposées cette année dans le cadre de l'exercice sur les typologies ont montré qu'apparemment, les OBNL peuvent être utilisés de toutes sortes de façons et à des fins différentes pour financer le terrorisme. Tout d'abord, les OBNL peuvent être utilisés par les terroristes et les organisations terroristes pour se procurer des fonds, comme ce fut le cas d'un grand nombre de OBNL de taille conséquente dont les actifs ont été gelés en vertu de la Résolution 1373 du Conseil de sécurité des Nations Unies. Souvent, mais pas toujours, ces organismes demandent, et obtiennent, un statut officiel d'organisation caritative ou une exonération fiscale. En outre, certaines de ces organisations auraient eu recours à des techniques assez dynamiques pour lever des fonds, faisant quelquefois appel à des dons du grand public, ou bien visant certains groupes-cibles, en particulier au sein de communautés ethniques ou religieuses spécifiques.

34. Un certain nombre d'experts ont insisté sur l'importance des *systèmes informels de collecte d'espèces* dans de nombreuses communautés ethniques ou religieuses, ainsi que sur les difficultés rencontrées pour les contrôler avec précision. Bien qu'il soit plus que probable que, dans leur grande majorité, ces fonds soit mobilisés et utilisés à des fins caritatives totalement légitimes, l'évident potentiel d'abus reste toutefois problématique. L'existence réelle ou feinte d'opérations de collecte de fonds peut également faciliter l'intégration des produits d'activités criminelles de groupes terroristes dans le « système financier légal ». Ces fonds sont ensuite présentés comme des fonds recueillis en toute légitimité à des fins caritatives pour un OBNL, et la procédure constitue donc à elle seule une forme de blanchiment de capitaux à des fins terroristes.

Exemple 5 : Collecte de fonds par l'intermédiaire d'un OBNL

Une organisation caritative dûment immatriculée, oeuvrant officiellement pour la protection de l'enfance, utilisait des cassettes vidéo dépeignant des « combattants de la liberté » religieux actifs dans différents pays, avec des images des atrocités commises à l'encontre des fidèle de cette religion. Les cassettes contenaient des appels à envoyer des dons à un numéro de boîte postale afin de contribuer à ce « combat ». Elles étaient apparemment largement diffusées dans des établissements religieux de la région. Le même numéro de boîte postale figurait dans d'autres appels relayés par des magazines publiant des articles rédigés par des extrémistes bien connus.

35. Les OBNL peuvent également être utilisés par les terroristes pour *faire circuler des fonds*. Dans ce cas, les terroristes profitent du fait que des opérations financières consistant à transférer des fonds d'un point géographique à un autre, souvent par-delà les frontières, sont considérées comme entrant dans le cadre normal des activités de certaines fondations ou organisations caritatives. Dans certains cas, la forme juridique et le but déclaré de l'OBNL semblent avoir été choisis avec soin de manière à échapper à toute réglementation et à tout contrôle (c'est le cas par exemple des associations culturelles établies dans certains pays par des communautés ethniques locales). Quelques exemples apparemment liés entre eux ont été cités par plusieurs délégations signalant l'établissement, dans différents pays, de réseaux de fondations apparentées au sein d'une communauté ethnique particulière et servant apparemment de cadre à des activités illégales de systèmes alternatifs de remise de fonds. Bien qu'il soit difficile de savoir si l'un quelconque de ces schémas est directement lié au financement du terrorisme, la structure des réseaux est intéressante en elle-même du fait de ses caractéristiques inhabituelles et de son potentiel de détournement. Ces exemples montrent également qu'il peut être extrêmement difficile de distinguer entre des transferts internes ou entre OBNL et la fourniture de services illégaux de remise de fonds. Ces « services alternatifs de remise de fonds » utilisent les comptes bancaires d'OBNL pour collecter des dépôts en espèces et soldent les comptes avec leurs contacts à l'étranger. Dans certains cas, ces transactions ont été considérées comme suspectes par les autorités compétentes du fait de la discordance entre les montants ainsi manipulés et la modestie des conditions de vie de la communauté particulière apportant son soutien financier à l'OBNL concerné.

Exemple 6 : Utilisation d'un OBNL pour transférer de l'argent à des personnes soupçonnées de terrorisme

La cellule de renseignements financiers d'un pays A a reçu des informations mises à jour portant sur la liste consolidée des personnes et entités visées par le Conseil de sécurité des Nations Unies. Une des organisations figurant sur cette liste exerçait ses activités sous différentes variantes du même nom dans un certain nombre de pays. Elle était décrite comme un OBNL exonéré d'impôt dont l'objet déclaré consistait à mener à bien des projets humanitaires dans le monde. Parmi les multiples emplacements cités dans la liste des Nations Unies pour les succursales de cette organisation, plusieurs avaient leur adresse dans le pays A.

La cellule de renseignements financiers a reçu une déclaration d'opération suspecte concernant un OBNL sis à l'une des adresses recensées dans la liste des Nations Unies. Cette déclaration faisait état de comptes bancaires et citait trois personnes possédant une participation de contrôle renvoyant tous à une adresse dans le pays A. L'une de ces personnes (M. A) avait une adresse qui correspondait à l'une de celles figurant sur la liste des Nations Unies, et les deux autres avaient leur adresse dans deux pays différents. Une enquête menée par la cellule de renseignements financiers a montré que M. A était lié à cette organisation, ainsi qu'à quatre autres

OBNL internationaux. Les rapports transmis à la cellule de renseignements financiers font état de virements électroniques multiples envoyés de lieux ayant un lien avec les succursales de l'organisation caritative susmentionnée et avec M. A.

Exemple 7 : Utilisation d'OBNL pour procéder à des transferts illégaux

Une enquête criminelle en cours sur un réseau de fondations (au moins 215 OBNL) créé par les membres d'une communauté d'immigrants a permis d'établir que ce réseau transférait régulièrement d'importantes sommes d'argent sur un petit nombre de comptes ouverts dans un autre pays. C'est le montant inhabituellement élevé des transactions par rapport à l'objet déclaré et aux activités des fondations qui a incité la banque à faire une déclaration d'opération suspecte. Après une première analyse, il est apparu évident que l'un des bénéficiaires des opérations effectuées par ces organisations était une entreprise figurant sur la liste de personnes visées par le Conseil de sécurité des Nations Unies. La cellule de renseignements financiers a transmis l'affaire aux autorités opérationnelles afin qu'elles poursuivent l'enquête.

Alors même que ces fondations avaient un objet ouvertement caritatif, la taille et la fréquence des virements (à la fois sur des comptes bancaires réguliers et par l'intermédiaire de services de transfert de fonds) étaient difficiles à justifier. Sur une période de trois ans, 35 OBNL ont ainsi envoyé à l'étranger plus de USD 160 millions. Le réseau était composé d'un nombre considérable de fondations réparties dans tout le pays, mais concentrées dans les villes où était implantée une large communauté d'immigrants en provenance du même pays. L'enquête criminelle en cours a déjà conclu qu'il était plus que probable que les OBNL servaient en fait de couverture à un système alternatif de remise de fonds. Bien qu'il soit encore trop tôt pour tirer une conclusion définitive sur l'origine et la destination des sommes transitant par ce réseau, on peut à tout le moins soupçonner que les fonds ont été levés au sein de cette communauté d'immigrants dans l'intention délibérée de soutenir des actes terroristes.

36. Enfin, les OBNL peuvent aussi être utilisées pour *fournir un soutien logistique direct* à des terroristes ou *servir de couverture à leurs activités*. Ce type d'abus est particulièrement évident parmi les OBNL qui ont plusieurs succursales opérant dans de nombreux pays ou territoires.

Exemple 8 : Utilisation d'un OBNL par des membres de sa direction pour financer le terrorisme

Un OBNL a été enregistré dans un pays X en qualité d'organisation caritative exonérée d'impôt ayant pour objet la réalisation de projets humanitaires dans le monde. Bien que cet OBNL ait été enregistré dans le pays X, il menait ses activités dans différents lieux sous des noms légèrement différents.

Des dossiers financiers et commerciaux ont été saisis au siège de l'OBNL et au domicile de son président et de l'un des membres de son conseil d'administration. Le même jour, le pays X a prononcé une décision de blocage des actifs et des dossiers de l'OBNL en attendant la poursuite des enquêtes. Onze moins plus tard, le pays X a communiqué le nom de cet OBNL aux Nations Unies afin qu'il soit visé par les résolutions concernées du Conseil de sécurité en raison du soutien apporté à une organisation terroriste.

Le président de l'OBNL a été condamné dans le pays X pour fraude et crime organisé, c'est-à-dire pour le détournement de plus de USD 315 000 de dons au profit d'organisations terroristes. Il a été prouvé qu'avant de se rendre coupable de ces infractions, l'OBNL avait fourni un soutien financier direct et indirect à des organisations terroristes.

Les différentes possibilités de détournement des OBNL

37. Les travaux menés cette année sur les OBNL ont permis de dégager une conclusion importante : les différentes catégories d'organismes à but non lucratif présentent des profils de risques différents, si bien que les caractéristiques inhabituelles qui peuvent être décelées et utilisées pour identifier une opération de financement du terrorisme varient. Il est important par exemple d'opérer une distinction entre les OBNL qui sont officiellement enregistrés en tant qu'organisations caritatives et utilisent

ensuite ce statut pour accéder à un éventail plus large de fonds et les OBNL qui exercent une fonction moins visible, évitant même quelquefois de se faire enregistrer ou de demander une exonération fiscale. Souvent, ces OBNL non enregistrés se financent auprès de communautés ethniques ou bien leur rendent des services. Ils se présentent souvent plutôt comme des associations culturelles ou encore des associations ou des fondations au service d'une communauté donnée plutôt que comme des organisations caritatives.

38. On peut également distinguer entre les OBNL qui opèrent au niveau international et ceux qui ont une fonction locale. On croit généralement, à tort, que les OBNL ne peuvent être utilisés de manière abusive que dans un contexte international en levant dans des pays donateurs des fonds qui seraient ensuite envoyés à des groupes terroristes dans des pays tiers. Or, bien que les OBNL à vocation internationale soient plus susceptibles d'être ainsi détournés, le financement du terrorisme peut également être le fait d'OBNL opérant à une échelle exclusivement nationale. Les pays confrontés à un problème de terrorisme intérieur savent d'expérience que des OBNL opérant à l'intérieur de leurs propres frontières ont déjà été détournés à des fins de financement de groupes terroristes locaux. Tout aussi erronée est l'idée selon laquelle le détournement d'OBNL par des terroristes serait exclusivement le fait d'extrémistes religieux.

39. Une autre distinction est par ailleurs possible, cette fois entre les différents degrés de complicité existant entre l'OBNL et ses donateurs. Si, dans la plupart des cas examinés cette année par les experts, on a pu établir que c'est la vénalité ou la complicité des dirigeants des OBNL qui avait facilité, voire motivé, les liens avec le financement du terrorisme, on peut aussi trouver des exemples d'OBNL largement innocents qui ont été exploités par quelques personnes infiltrées ayant réussi à ponctionner ou à détourner leurs fonds. De plus, il peut également arriver qu'un OBNL soit victime d'une organisation bénéficiaire sans lien avec lui, ou encore d'une de ses succursales. On a même relevé des cas de « contrefaçon » d'appels de fonds, où le nom d'un OBNL existant était utilisé à son insu comme couverture pour se procurer illégalement des fonds.

Repérer le financement du terrorisme dans le secteur des OBNL

40. Compte tenu des typologies définies, les experts sont parvenus à la conclusion que la méthode ayant la meilleure chance de succès pour détecter d'éventuels liens entre le financement du terrorisme et les OBNL était celle mise en œuvre par les services de renseignements ou de police, grâce à des mises en relation avec d'autres OBNL (pour des motifs opérationnels, financiers ou du fait de l'existence de dirigeants ou de personnel communs) ou à des liens avec des personnes déjà soupçonnées d'activités terroristes ou ayant pour objectif de financer le terrorisme. Il peut arriver dans certains cas que les administrateurs ou les dirigeants d'un OBNL aient déjà un passé en relation avec des mouvements extrémistes, voire aient été mêlés à des affaires criminelles ou en liaison avec le terrorisme. Dans d'autres cas, il est possible d'établir des liens avec des organisations terroristes bien connues ou avec d'autres OBNL figurant déjà sur les différentes listes de personnes ou d'entités dressées par les Nations Unies ou par des pays à titre individuel. Les préoccupations et indications du public sur l'implication possible d'un OBNL dans des activités douteuses peuvent également jouer un rôle dans la détection d'abus éventuels.

41. L'établissement de déclarations d'opérations inhabituelles suspectes par les institutions financières, et l'analyse qui en est faite ensuite par les cellules de renseignements financiers ou les autorités opérationnelles, peuvent également contribuer dans une large mesure à faire émerger certains soupçons de détournement d'un OBNL par des terroristes. Dans certains pays, des déclarations d'opérations suspectes liées à une activité inhabituelle d'un OBNL ont effectivement abouti au lancement d'une enquête, tandis que dans d'autres, le système de déclarations et les analyses effectuées par la cellule de renseignements financiers ont contribué à de nouvelles avancées dans des enquêtes en cours.

42. Il ne semble pas que les activités de contrôle incombant aux autorités de surveillance ou aux administrations fiscales chargées des OBNL aient permis de mettre à jour des affaires de financement

du terrorisme au sein du secteur caritatif. Cela étant, ces autorités ont quelquefois joué un rôle important pour obtenir des informations, parce qu'elles étaient en mesure de poser d'autres questions ou d'inspecter des entités et/ou d'échanger ces renseignements avec les autorités opérationnelles.

43. Les experts sont tombés d'accord sur le fait que chacun de ces mécanismes de détection avait une fonction complémentaire qu'il était possible d'exercer ou d'améliorer collectivement. La diversité des mécanismes de détection et des sources d'informations possibles concernant le détournement potentiel des organisations caritatives à des fins terroristes souligne l'importance de la conclusion d'accords efficaces d'échange de renseignements, au sein-même des administrations et entre elles.

Signaux d'alerte

44. Outre les liens avec des personnes soupçonnées de terrorisme, des organisations terroristes et d'autres OBNL suspects, les experts ont également identifié un certain nombre de caractéristiques individuelles inhabituelles, sorte de « clignotants rouges », dans les exemples examinés au cours de l'exercice de cette année sur les typologies. Certaines de ces caractéristiques inhabituelles pourraient se révéler particulièrement utiles aux institutions financières, d'autres le seront sans doute davantage pour les autorités chargées de la surveillance ou des enquêtes.

Caractéristiques financières spécifiques :

- Discordance entre les donateurs prétendus et les montants levés ou transférés, par exemple dans les cas où des sommes très importantes sont censées être collectées au sein de communautés ayant un niveau de vie très modeste.

- Incohérence entre le type et la taille des transactions financières d'une part et l'objet déclaré et les activités de l'OBNL d'autre part, par exemple (comme dans l'exemple cité plus haut) une association culturelle qui, après dix années d'existence, ouvre un compte bancaire pour gérer les produits générés par un festival de musique et y dépose une somme d'argent d'un montant disproportionné.

- Augmentation soudaine de la fréquence et du montant des mouvements d'un compte appartenant à un OBNL, ou inversement, à savoir que l'OBNL conserve apparemment des fonds sur son compte pendant une très longue période.

- Transactions en espèces d'un montant significatif et inexpliqué par un OBNL.

- Absence de contributions de la part de donateurs résidant dans le pays d'origine de l'OBNL.

Autres caractéristiques :

- Existence d'administrateurs étrangers, en particulier dans les cas de sorties de fonds importantes à destination du pays d'origine de ces administrateurs, et surtout si ce pays est une destination à haut risque.

- Existence d'un grand nombre d'OBNL avec des relations inexpliquées : par exemple, plusieurs OBNL se transfèrent mutuellement de l'argent, ou bien ont la même adresse, les mêmes dirigeants ou le même personnel, ou bien encore un grande nombre d'OBNL sont liés à la même communauté et ont recours aux services d'un même « ouvreur de porte ».

- Existence d'OBNL ayant des ressources négligeables par rapport à leur objet déclaré ou à leurs flux financiers, ou bien encore n'ayant apparemment pas ou peu de personnel, de bureaux convenables ou de numéro de téléphone.

- Des activités exercées dans des pays à haut risque, ou bien des transactions à destination ou en provenance de ces mêmes pays, peuvent également être considérées comme un motif de vigilance accrue de la part des institutions financières. Elles peuvent également servir de motif au déclenchement d'une surveillance plus étroite de la part des autorités de surveillances ou d'autres autorités compétentes.

Conséquences au plan de l'action publique

Diversité des systèmes et des conceptions de surveillance

45. Les experts participant à l'exercice sur les typologies de cette année et plus spécifiquement à l'atelier sur les OBNL sont parvenus à un consensus sur le fait que des mesures supplémentaires devront sans doute être élaborées pour réduire la vulnérabilité des OBNL au regard du financement du terrorisme. L'ampleur et la nature de ces mesures restent toutefois à définir. L'absence d'orientation claire sur ce point reflète en partie le fait qu'il existe de grandes différences entre les pays dans la manière dont ils exercent la surveillance du secteur des OBNL et dont ils en assurent la transparence. Certains pays par exemple ont une longue tradition de surveillance active des OBNL par les pouvoirs publics, tandis que d'autres mettent davantage l'accent sur les enquêtes criminelles et les obligations de conservation des documents. D'autres encore ont mis en place des systèmes réglementaires d'envergure, prévoyant notamment des obligations de conservation des documents et de déclaration d'opérations suspectes, le recours à des réviseurs comptables externes, la délivrance d'autorisations, le recours obligatoire à des comptes bancaires autorisés, des autorisations pour effectuer des transactions internationales et des obligations détaillées de vigilance vis-à-vis de la clientèle (en l'occurrence les OBNL) pour les banques..

46. Ces différences d'approche d'un pays à l'autre semblent le plus souvent liées aux différentes conceptions concernant le rôle de la puissance publique dans la réglementation des organisations caritatives et autres types d'OBNL. Certains pays estiment que la protection des donateurs légitime une réglementation et une surveillance étendue de la part des pouvoirs publics. D'autres sont d'avis que la protection des donneurs incombe avant tout à ceux qui versent des contributions aux OBNL, et dans ce cas, ce sont des organisations de surveillance privées (du style des « watchdog organisations »), etc. qui sont chargés de cette surveillance.

47. Dans de nombreux pays, les OBNL ayant obtenu de l'administration fiscale un statut d'exonération totale ou partielle sont soumis à une forme ou une autre de réglementation et de surveillance. Dans certains cas, cette administration joue même quelquefois un rôle important et actif dans la surveillance de ces organisations. Par exemple, le fisc peut demander des rapports annuels détaillés à chaque OBNL enregistré, et rendre ces informations publiques sur demande. Dans d'autres pays, la réglementation et la surveillance exercées par les pouvoirs publics vise essentiellement à protéger l'intégrité de certains types d'entités juridiques qui disposent d'une autorisation spécifique pour gérer d'importantes sommes à vocation caritative.

48. Enfin, il existe évidemment une autre raison pour accroître la surveillance réglementaire du secteur des OBNL, à savoir empêcher qu'il ne soit détourné à des fins criminelles, non seulement pour financer le terrorisme, mais également dans un but de blanchiment de capitaux et de fraude. Quelle que soit l'approche retenue, il semble qu'il subsiste des lacunes significatives dans les systèmes adoptés par la plupart des pays. Les experts ont ainsi identifié un certain nombre de contraintes importantes susceptibles d'empêcher les pays ou les territoires de réduire efficacement la menace que représente l'usage abusif des OBNL à des fins de financement du terrorisme et autres activités criminelles.

49. La plupart des pays ne peuvent consacrer qu'une part limitée de leurs ressources à la réglementation et à la surveillance du secteur des OBNL, lequel recouvre dans certains cas des centaines de milliers d'organisations qui peuvent avoir entre leurs mains un pourcentage important du PIB d'un pays. Cette observation est particulièrement valable pour nombre de pays destinataires de

dons ou de pays en développement, dans lesquels des OBNL de toutes tailles, ayant souvent une assise communautaire, jouent un rôle crucial au sein de l'économie. Il arrive quelquefois que dans ces pays, le secteur des OBNL ait un poids économique plus lourd que le secteur public.

50. Dans la plupart des pays, un très fort pourcentage (qui peut aller jusqu'à 90%) du total des OBNL est constitué d'organisations de taille très réduite. Il est parfois très difficile à celles-ci de supporter la charge administrative considérable qui serait nécessaire pour se conformer à une réglementation administrative détaillée. Même dans les plus grandes organisations, il y a des limites à ce que l'on peut considérer comme une charge administrative raisonnable, dans la mesure où les ressources des OBNL sont par nature modestes comparées aux services souvent essentiels qu'ils rendent. De plus, il existe dans certains pays des dispositions juridiques, voire constitutionnelles, qui empêchent ou limitent l'imposition d'obligations réglementaires à certaines catégories d'OBNL. C'est le cas par exemple des dispositions relatives à la liberté d'association ou du statut spécial accordé à des organisations à vocation religieuse.

Conclusions et questions devant faire l'objet d'un suivi

51. Les experts participant à l'exercice sur les typologies de cette année sont parvenus à un consensus sur le fait que quelle que soit l'approche retenue, la réglementation ou la surveillance exercées par les pouvoirs publics devait prendre en compte l'élément de risque. Toute instance de surveillance (qu'il s'agisse d'une autorité de réglementation en tant que telle ou de l'administration fiscale) devrait avoir une mission bien ciblée et se concentrer sur les domaines présentant des risques élevés. Pour certains experts, la fonction de surveillance est sans doute plus utile lorsqu'elle permet d'obtenir des informations sur une affaire de financement du terrorisme aux tous premiers stades d'une enquête alors qu'il n'existe encore pas de motifs suffisants pour engager une enquête criminelle que lorsqu'elle permet d'obtenir des informations isolées. Pour d'autres, la surveillance exercée par les pouvoirs publics a une fonction évidente de prévention et d'information au sens où elle impose une vigilance accrue pour certaines catégories d'OBNL à haut risque. Quoi qu'il en soit, tous ont admis que le fait d'avoir le pouvoir et les moyens de réagir à des caractéristiques suspectes ou inhabituelles d'un OBNL avant qu'il y ait des motifs suffisants pour lancer une enquête criminelle constituait sans doute l'un des éléments les plus cruciaux d'un système efficace de lutte contre le détournement du secteur des OBNL.

52. Quelle que soit l'approche retenue pour surveiller les OBNL, il risque néanmoins de subsister dans les systèmes de nombreux pays des exceptions ou des lacunes qui empêchent de réduire réellement la vulnérabilité du secteur dans son ensemble. Par exemple, certains pays n'ont quelquefois pas les moyens de surveiller les OBNL qui ne demandent pas à être exonérés d'impôts, ni les organisations religieuses, ni les OBNL constitués sous certaines autres formes juridiques non réglementées. Il est donc nécessaire d'examiner dans quelle mesure ces différents compartiments du secteur des OBNL sont susceptibles d'être détournés de leur objet à des fins de financement du terrorisme ou à d'autres fins, puis de trouver d'autres solutions permettant de garantir la transparence et, si nécessaire, l'accès aux autorités compétentes. L'une des solutions citées par un pays consisterait à obliger les OBNL à s'enregistrer auprès de l'administration fiscale pour pouvoir ouvrir un compte bancaire.

53. Les experts sont d'avis que pour pouvoir obtenir et approfondir les informations sur les OBNL, il est important de continuer à élaborer ou à améliorer des mécanismes et des dispositifs d'échange de renseignements, au plan national et international. Afin de faciliter la coopération au niveau national, les participants se sont montrés très favorables à l'idée de créer des « groupes nationaux d'action» composés de représentants des autorités opérationnelles, des services de renseignement et de sécurité, de membres du personnel des cellules de renseignements financiers, ainsi que de représentants des autorités de surveillance des OBNL et des administrations fiscales. De tels groupes d'action pourraient : (i) étudier et évaluer le risque de financement du terrorisme dans le secteur des OBNL ; (ii) afin de limiter ce risque, recommander que soit élaboré un mécanisme de surveillance approprié, efficace mais équilibré, ou qu'un tel mécanisme soit amélioré s'il existe déjà, et (iii) échanger des

renseignements sur des activités de financement du terrorisme, potentielles ou suspectées qui se produisent dans ce secteur.

54. En ce qui concerne les échanges de renseignements et la coordination au plan international, les experts ont souligné combien il importait que les différentes autorités, homologues ou non (c'est-à-dire pas uniquement entre cellules de renseignements financiers par exemple, mais également entre cellules de renseignements financiers et autorités réglementaires ou opérationnelles) échangent rapidement leurs informations et fassent preuve d'initiative. Ce type d'échange viendrait en complément des échanges plus formels, en particulier lorsqu'il existe de fortes présomptions que l'on soit en présence de groupes actifs au niveau international et de relations possibles avec des OBNL spécifiques à l'étranger. Des organisations internationales capables de comparer différentes bases de données nationales pourraient également jouer un rôle très utile à cet égard.

55. Il conviendra également de veiller avec un soin tout particulier à lever les obstacles qui empêchent de retracer et de vérifier l'utilisation des ressources des OBNL dans les pays tiers (activités ou relations à l'étranger). Ceci est particulièrement délicat dans les zones en difficulté ou dans les endroits qui sont le théâtre de conflits. Pour résoudre ce problème, un certain nombre de pistes ont été explorées, notamment : (i) la nécessité d'un renforcement de la coopération entre les autorités du pays du donateur et du pays du destinataire des fonds ; (ii) la possibilité de coordonner et d'échanger les informations recueillies à l'occasion de contrôles sur site occasionnels réalisés à l'étranger ; (iii) la possibilité d'acheminer des fonds par le biais d'organisations locales explicitement autorisées et contrôlées ; (iv) l'élaboration d'un modèle-type de procédures fiables pour les transactions et opérations internationales (examiner les procédures des OBNL les plus importants et les plus solidement établis dans chaque pays d'origine des fonds et dans chaque pays destinataire) ; (v) la possibilité de renverser la charge de la preuve dans certaines circonstances (les OBNL situés dans les pays donateurs prouvant que les activités et transactions effectuées à l'étranger, éventuellement par le biais d'OBNL locaux, sont menées conformément à leur objet déclaré et à leur statut), et (vi) la possibilité d'obliger les OBNL à obtenir des licences assorties d'obligations de vigilance accrue avant de les autoriser à exercer leurs activités dans certains territoires ou zones présentant un risque élevé de conflit ou de terrorisme. Aucune de ces possibilités n'est censée décharger les pays de destination des fonds de toute responsabilité en matière de surveillance du secteur des OBNL, mais chacune des propositions constitue un moyen d'améliorer la protection de ce secteur en imposant des obligations supplémentaires au pays du donateur ou à l'OBNL. Elles pourraient en outre contribuer à assurer une protection suffisante contre le détournement des ressources dans les zones géographiques où le contrôle exercé par les pouvoirs publics est relativement faible, en particulier dans les zones de conflit.

56. Des travaux supplémentaires devront être menés de façon à ce qu'il soit possible d'utiliser de manière optimale le système de déclaration des opérations suspectes ou inhabituelles pour repérer un éventuel détournement des OBNL. Il faudra également poursuivre les études sur les « signaux d'alerte » ainsi que sur les meilleures pratiques de vigilance vis-à-vis des OBNL. Enfin, il est important que tous les pays entament des discussions avec leurs OBNL afin de garantir leur compréhension et coopération mutuelle dans la lutte contre le financement du terrorisme. Il est également fondamental que les pays utilisent au maximum les connaissances et le savoir-faire acquis au sein du secteur des OBNL pour définir des mesures et obligations réalistes et efficaces et identifier les pratiques exemplaires appropriées.

III. LES RISQUES DE BLANCHIMENT DANS LE SECTEUR DE L'ASSURANCE

57. Selon certaines sources, le secteur des assurances génère dans le monde des primes de l'ordre de USD 2 400 à 2 600 milliards[3]. Ce secteur propose des produits de transfert de risques, d'épargne et de placement à un large éventail de clients allant des particuliers aux grandes entreprises multinationales en passant par les administrations publiques. Le secteur des assurances est lui-même divers : on y distingue en effet trois grandes branches (selon les types de produits offerts) : l'assurance non vie, l'assurance-vie et la réassurance. Ces activités, comme tout autre service financier, sont exposées au risque de blanchiment, et les participants à de précédents exercices du GAFI sur les typologies (en particulier celui de l'année dernière) ont fait état d'affaires dans lesquelles certains produits d'assurance avaient été utilisés pour blanchir de l'argent. Pour cette raison, le GAFI a décidé de retenir l'assurance comme thème du troisième atelier organisé dans le cadre de l'exercice de cette année.

58. Pour les institutions financières, les paiements en provenance de compagnies d'assurance sont monnaie courante. L'argent est supposé « propre » et les versements n'attirent pas l'attention. Si des blanchisseurs arrivent à placer de l'argent dans une police d'assurance, cela signifie qu'ils ont déjà bien progressé dans l'empilage et l'intégration des fonds dans le système financier international.

59. Les experts considèrent que l'assurance est potentiellement vulnérable au blanchiment de capitaux du fait de la taille du secteur, de la disponibilité et de la diversité de ses produits et de la structure-même de ses activités. En ce qui concerne ce dernier point, il importe de signaler que dans certains pays ou territoires, l'assurance est souvent une activité transnationale et que dans la majorité des cas, ses produits sont distribués par l'entremise de courtiers ou autres intermédiaires qui ne sont pas nécessairement affiliés à la compagnie qui les conçoit, ou qui ne sont pas placés sous son contrôle ou sous sa surveillance. En outre, comme le bénéficiaire d'un produit d'assurance n'est souvent pas le même que le souscripteur de la police d'assurance, il est quelquefois difficile de déterminer à quel moment et à l'encontre de quelle personne il est nécessaire d'accomplir le devoir de vigilance vis-à-vis de la clientèle (doit-on vérifier uniquement l'identité du souscripteur, ou bien également celle du bénéficiaire ?).

60. Afin de réduire les risques inhérents aux activités d'assurance, de nombreux pays ont choisi de soumettre certaines branches de ce secteur à des obligations formelles de lutte contre le blanchiment, par exemple le devoir de vigilance vis-à-vis de la clientèle et l'obligation de déclaration des opérations suspectes. Il existe en outre des normes internationales de lutte contre le blanchiment proposées par les assureurs eux-mêmes et diffusées par l'intermédiaire de l'Association Internationale des services de Contrôles des Assurances (AICA ou *International Association of Insurance Supervisors, IAIS*)[4]. Les lignes directrices de lutte contre le blanchiment publiées par l'IAIS à l'intention des sociétés d'assurance recensent ainsi les principes et procédures clés propres à cette industrie, notamment le respect des obligations de vigilance vis-à-vis de la clientèle et la mise en œuvre de programmes de formation destinés au personnel.

61. Au cours de l'exercice de cette année sur les typologies, les participants se sont penchés sur les risques, les tendances et les vulnérabilités du secteur des assurances au regard du blanchiment et tenté de cerner la nature et l'ampleur d'un problème de blanchiment éventuel, afin d'identifier les catégories d'assurance qui sont le plus menacées par le phénomène du blanchiment de capitaux.

Typologies

62. Un certain nombre de méthodes de blanchiment ont été repérées dans le secteur des assurances, et certaines d'entre elles avaient déjà été recensées les années précédentes. Au stade du placement par

[3] OCDE (2003), *Annuaire des statistiques d'assurance 1994 - 2001*, page 2; et "Sigma Insurance Research Paper 8", *World Insurance in 2002*, page 26.

[4] Pour toute information complémentaire sur l'AICA, on pourra consulter son site Internet www.iaisweb.org.

exemple, les assurances sont utilisées par le simple achat en espèces de produits d'assurance à l'aide de produits dérivés d'activités criminelles. Dans ce cas, les blanchisseurs profitent du fait que les produits d'assurance sont souvent vendus par des courtiers, c'est-à-dire des agents n'agissant pas directement sous le contrôle ou la surveillance de la compagnie émettrice des produits. Ainsi, les blanchisseurs sont à la recherche de courtiers qui ne connaissent pas les procédures requises, ou qui ne s'y conforment pas, ou encore qui omettent simplement de consigner ou de déclarer des informations relatives à des cas possibles de blanchiment.

Exemple 9 : Utilisation d'une police d'assurance pour blanchir de l'argent

Un blanchisseur a souscrit une assurance maritime IARD pour un navire fictif. Il a versé de grosses primes et corrompu les intermédiaires, si bien que des sinistres étaient régulièrement déclarés et remboursés. Toutefois, il veillait très soigneusement à ce que les sinistres soient inférieurs aux primes, de manière à ce que l'assureur puisse dégager un bénéfice raisonnable de la police d'assurance.

De cette façon, le blanchisseur arrivait à recevoir des chèques de remboursement de sinistre qui servaient à blanchir les fonds. En effet, ceux-ci venaient apparemment d'une compagnie d'assurance honorable, et bien peu de personnes ayant vu le nom de cette compagnie sur les chèques ou virements se sont interrogés sur l'origine de ces fonds.

Exemple 10 : Blanchiment de sommes versées par une compagnie d'assurance

La police d'assurance du pays A a découvert une affaire de trafic de voitures volées dans laquelle les malfaiteurs provoquaient des accidents dans un pays B afin de pouvoir réclamer des dommages. Les produits étaient ensuite blanchis via des sociétés de travaux publics. Le réseau était constitué de deux équipes opérant dans deux régions différentes du pays A. Des véhicules de luxe étaient volés et envoyés dans le pays B après avoir été équipés de fausses plaques d'immatriculation. Un contrat d'assurance était souscrit pour ces véhicules dans le premier pays. Dans le pays B, les voitures étaient délibérément déclarées irrécupérables et des épaves portant de faux numéros d'immatriculation étaient rachetées à l'aide de documents d'identité falsifiés afin de demander le remboursement des sinistres à la compagnie d'assurance du pays A.

Environ une centaine de voitures de luxe volées ont ainsi été utilisées pour réclamer des dommages au titre d'accidents intentionnels ou simulés qui étaient ensuite frauduleusement déclarés aux compagnies d'assurance. La perte totale a dépassé les USD 2,5 millions. Le pays dans lequel les accidents se « produisaient » avait été choisi parce que sa législation nationale prévoyait un remboursement rapide des dommages.

A réception des remboursements, les faux déclarants remettaient 50 pour cent de la somme en espèce au chef du réseau qui investissait l'argent dans le pays B. Les enquêtes ont montré que des transferts bancaires représentant plus de USD 12 500 par mois avaient été effectués entre ses comptes et le pays en question. L'argent était investi dans l'achat de nombreux véhicules de travaux publics et dans la constitution d'entreprises de ce secteur dans le pays B. Les enquêtes ont également révélé que le chef du réseau possédait un entrepôt dans lequel les véhicules de luxe utilisés pour ses trafics étaient stockés. Il a été par ailleurs établi que cette personne était en relations d'affaires avec un promoteur, ce qui semblerait indiquer que le réseau cherchait à placer une partie de ses gains dans l'immobilier.

63. Les exemples cités cette année au cours de l'exercice sur les typologies apportent semble-t-il une nouvelle démonstration du fait qu'il existe un certain nombre de « signaux d'alerte » potentiels quant à la possibilité d'une opération de blanchiment, notamment si l'on se rend compte que le souscripteur d'une police d'assurance est plus intéressé par les conditions d'annulation que par les avantages offerts par son contrat. L'utilisation d'espèces et/ou le versement de primes uniques importantes, comme, d'une manière générale, l'utilisation de gros volumes d'espèces pour effectuer un règlement, devraient être considérés comme suspects et comme une tentative potentielle de placement de fonds d'origine criminelle dans le système financier par le biais de produits d'assurance.

64. La réception de primes provenant d'intermédiaires financiers extraterritoriaux et/ou soumis à une réglementation peu contraignante, voire non réglementés, peut également être le signe du recours potentiel à des produits d'assurance à des fins de blanchiment. Il y a un risque à traiter avec des intermédiaires non réglementés et à en recevoir des paiements, car ils omettent souvent de s'assurer que les mesures de vigilance à l'égard de la clientèle ont bien été prises en relation avec les fonds investis dans leurs polices d'assurance. Un certain nombre d'experts ont fait remarquer que dans de nombreux pays, les compagnies d'assurance prennent des mesures de vigilance accrues afin de faire face à ce risque spécifique.

65. Une autre méthode de blanchiment au moyen de polices d'assurance, en particulier celles qui servent de supports à des placements, consiste, pour les blanchisseurs, à faire un ou plusieurs versements excédentaires sur des primes et à demander ensuite que le trop-versé soit remboursé à un tiers. Il conserve ainsi sa police d'assurance en tant que produit de placement, et peut en même temps blanchir des fonds grâce aux contributions excédentaires/remboursements.

Exemple 11 : Utilisation de l'assurance pour blanchir des capitaux

Dans plusieurs pays, des clients avaient recours aux services d'un intermédiaire pour souscrire des polices d'assurance. L'identification était faite au moyen d'une carte d'identité, mais il était impossible aux compagnies locales de vérifier ces informations, et elles s'en remettaient à l'intermédiaire pour exercer les mesures de vigilance.

Les polices d'assurance étaient souscrites et les paiements effectués par les intermédiaires auprès des compagnies locales. Ensuite, après quelques mois, les compagnies recevaient une notification des clients indiquant que les circonstances avaient changé, qu'ils devaient résilier la police d'assurance déficitaire, et qu'ils en demandaient en conséquence le remboursement (par chèque).

D'autres fois, la police d'assurance était conservée pendant quelques années avant d'être résiliée en demandant son remboursement au profit d'un tiers. Le chèque de remboursement était ensuite souvent traité par une institution financière locale qui ne posait aucune question, puisque le chèque émanait d'une autre institution locale honorablement connue.

66. Les changements fréquents de bénéficiaires, l'utilisation de la police d'assurance comme actif au porteur ou comme garantie dans le cadre d'une opération plus vaste de blanchiment, conjugués à une résiliation anticipée des polices d'assurance à usage de placement, en particulier lorsque de telles pratiques sont contraires à la logique économique, ont été également cités comme indicateurs potentiels de blanchiment par certains pays membres[5].

67. Une partie des indicateurs de blanchiment potentiel cités ici sont relativement faciles à identifier pour un assureur ou un intermédiaire diligent. Dans certains cas, il peut y avoir des motifs légitimes à de telles actions. Toutefois, dans plusieurs exemples de blanchiment avéré fournis par les experts, plusieurs indicateurs étaient présents simultanément. Il convient de signaler ici que nombre d'entre eux semblent concerner des produits d'assurance-vie servant de placements. Comme indiqué plus haut, ces exemples portent sur l'utilisation de produits d'assurance comme produits d'épargne ou de placement dans lesquels le versement d'argent sale est suivi de la récupération de tout ou partie des fonds sous la forme d'un remboursement d'apparence légitime.

[5] On trouvera aux pages 19 et 20 des lignes directrices de lutte contre le blanchiment de l'AICA à l'intention des contrôleurs et compagnies d'assurance d'autres indicateurs potentiels de blanchiment dans le secteur de l'assurance ; voir le site http://www.iaisweb.org/02money.pdf.

Exemple 12 : Des membres d'un réseau de criminalité organisée blanchissent de l'argent grâce à des polices d'assurance-vie

Dans le pays X, des agents des douanes ont lancé une enquête qui a permis de révéler qu'une organisation de trafic de drogue avait utilisé le secteur de l'assurance pour blanchir les produits de ses activités. Les enquêtes menées par les autorités opérationnelles de plusieurs pays ont montré que les trafiquants blanchissaient les fonds par l'entremise de la compagnie d'assurance Z, située dans un territoire offshore.

La compagnie d'assurance Z propose des produits d'investissement qui s'apparentent à des fonds communs de placement. Le taux de rendement était indexé sur de grands indices boursiers internationaux, si bien que ces polices d'assurance pouvaient servir de placements. Les souscripteurs investissaient un maximum d'argent dans la police d'assurance, et en versaient ou en retiraient afin de couvrir le coût des pénalités de retrait anticipé. Les fonds sortaient alors sous la forme d'un virement ou d'un chèque émanant de la compagnie d'assurance, ce qui leur conférait une apparence de « propreté ».

A ce jour, l'enquête a montré que plus de USD 29 millions avaient été blanchis par ce biais. En outre, grâce aux efforts déployés conjointement par les agents des douanes du pays Y (pays d'origine des stupéfiants) et du pays Z, plusieurs avis de recherche et mandats d'arrêt ont pu être exécutés concernant les personnes ayant participé aux activités de blanchiment par l'intermédiaire de la compagnie d'assurance Z.

68. Les experts participant à l'atelier sur l'assurance ont par ailleurs souligné que les autres produits d'assurance pouvaient être pareillement vulnérables au blanchiment lorsqu'il y a recours quasi-exclusif à des intermédiaires (là encore, des courtiers ou des agents qui ne sont pas liés à la compagnie qui propose les produits). Le risque est encore bien plus élevé si l'on tient compte du manque relatif d'obligations ayant trait à la lutte contre le blanchiment et autres réglementations applicables à ce secteur.

L'assurance et les déclarations d'opérations suspectes

69. Les experts participant cette année à l'exercice sur les typologies ont souligné le nombre relativement minime de déclarations d'opérations suspectes générées par le secteur des assurances. Cette observation semble avérée pour la majorité des participants à l'atelier et ce, malgré le fait que le secteur de l'assurance est soumis à l'obligation de déclarer les opérations suspectes depuis déjà un certain nombre d'années dans de nombreux pays. De plus, le nombre de déclarations ne correspond pas forcément à la taille relative du secteur par rapport au secteur financier dans son ensemble. Ainsi, certains pays possédant un secteur de l'assurance très développé ne font état que d'un nombre très faible de déclarations d'opérations suspectes en liaison avec l'assurance, en dépit d'obligations rigoureuses en la matière.

70. Les experts se sont demandé si un nombre relativement faible de déclarations d'opérations suspectes et d'affaires impliquant du blanchiment en liaison avec l'assurance était le signe que le secteur des assurances n'est pas tellement utilisé par les blanchisseurs, ou bien si les affaires de blanchiment échappaient simplement à toute détection. De l'avis de certains, étant donné la taille du secteur des assurances, les possibilités de blanchiment qu'il offre sont trop grandes pour que les blanchisseurs les ignorent. D'autres en revanche ont avancé que le niveau élevé de la surveillance exercée dans leur pays, conjuguée à la suppression des polices d'assurance au porteur, avaient quelque peu minimisé le risque potentiel. Cela étant, l'expérience acquise dans d'autres branches du secteur financier montre que ce sont les secteurs du système financier où les procédures anti-blanchiment ne sont pas mises en œuvre de manière cohérente qui présentent le plus de risque d'être exploités à des fins de blanchiment.

Conséquences au plan de l'action publique

71. Le montant des opérations de blanchiment détectées au sein du secteur des assurances paraît très faible comparé à la taille de ce secteur. Néanmoins, les experts estiment que le secteur des assurances

reste vulnérable. Il est possible que des montages destinés à blanchir des capitaux passent inaperçus du fait de la conjonction de plusieurs facteurs : nature-même de l'activité (dépendance par rapport à des courtiers pour la distribution des produits), mise en œuvre fragmentaire et incomplète des règles et réglementations de lutte contre le blanchiment, et absence d'engagement au niveau de l'ensemble des opérateurs de l'assurance pour réagir à ce risque. Dans un premier temps, il sera vraisemblablement nécessaire de mieux comprendre comment et dans quelle mesure les différentes parties du secteur des assurances peuvent être utilisées par les blanchisseurs.

72. Afin de combler les lacunes que génère une application inadéquate des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme, il sera sans doute nécessaire de déployer des efforts supplémentaires pour mettre en œuvre les mesures existantes. Il faudrait améliorer l'échange de renseignements sur les typologies relatives à l'assurance, à la fois au sein du secteur lui-même et entre les assureurs, les services opérationnels et les autorités de surveillance. On pourrait aussi encourager les autorités opérationnelles et les autres services chargés des enquêtes à identifier d'éventuelles typologies de blanchiment relevées au cours d'autres enquêtes, par exemple les liens avec les fraudes aux déclarations de sinistres.

73. Les experts ont conclu que c'est probablement au stade de l'intégration et de l'empilage du cycle de blanchiment que le secteur des assurances était le plus vulnérable. Or, c'est à ce stade que les indicateurs sont le moins nets, ou qu'il est nécessaire de mettre en œuvre des mesures de vigilance relatives à la clientèle différentes ou d'une autre ampleur si l'on veut pouvoir détecter une opération de blanchiment. De fait, les procédures de base d'identification de la clientèle sont sans doute insuffisantes si elles ne sont pas doublées de mesures de vigilance plus détaillées.

74. La nature du risque de blanchiment inhérent au secteur des assurances semble différente de celle observée dans le reste du secteur financier ; en conséquence, il sera sans doute nécessaire de mettre au point des mesures de lutte contre le blanchiment spécifiques à ce secteur. Les experts ont également conclu que des travaux complémentaires devraient être menés pour mieux comprendre et définir les vulnérabilités spécifiques à l'ensemble du secteur des assurances (et pas uniquement pour la seule assurance-vie).

IV. LES PERSONNES POLITIQUEMENT EXPOSÉES

75. Lors de son examen de la vulnérabilité des activités de banque privée en 2001, le GAFI s'est penché sur la question des personnes politiquement exposées et des risques qu'elles représentent pour le secteur financier. La presse fait fréquemment état de nouvelles révélations concernant des personnes politiquement exposées soupçonnées d'être impliquées dans des affaires de criminalité financière, en particulier de corruption. Après la publication de la version révisée des Quarante recommandations, qui contient des mesures renforcées visant spécifiquement les risques liés aux personnes politiquement exposées, le GAFI a décidé d'inscrire également un bref examen de cette question au programme de l'exercice de cette année sur les typologies. Cette question a donc été examinée au cours de la réunion des experts au complet, et quelques premières conclusions ont ainsi pu être dégagées.

76. *Les personnes politiquement exposées, ou PPE,* sont des personnes qui exercent (ou ont exercé) d'importantes fonctions publiques dans un pays donné, par exemple de chefs d'État ou de gouvernement, d' hommes politiques de haut rang, de hauts fonctionnaires, de magistrats ou militaires de haut rang, de dirigeants d'entreprises publiques ou encore de dirigeants de partis politiques. Du fait du statut spécial qui est le leur, politiquement au sein de leur pays d'origine, ou diplomatiquement lorsqu'ils sont en poste à l'étranger, une certaine discrétion est souvent laissée aux institutions financière eu égard aux opérations financières menées par de telles personnes, ou pour leur compte. Si une PPE se trouve impliquée dans un activité criminelle de quelque nature que ce soit, cette discrétion traditionnelle eu égard à leurs activités financières se transforme souvent en obstacle lorsqu'il s'agit de déceler l'activité à laquelle ils ont pris part, ou d'enquêter à son sujet.

77. Les documents présentés au cours de la réunion des experts et les contributions écrites soumises par les participants appellent plusieurs observations. Premièrement, les fonds qu'une PPE peut tenter de blanchir n'ont pas uniquement pour origine des pots-de-vin, commissions illégales ou autres produits directement issus de la corruption : il peuvent également provenir de détournements, voire de vol pur et simple d'actifs publics ou de fonds appartenant à des partis politiques ou à des syndicats, ou bien encore de fraude fiscale. Dans certains cas, il peut même arriver qu'une PPE soit directement impliquée dans d'autres types d'activités illégales, criminalité organisée ou trafic de drogue par exemple. Apparemment, ce sont les PPE issues de pays ou de régions du monde où la corruption est endémique, organisée et systémique qui présentent les risques potentiels les plus élevés, mais il faut rappeler qu'il existe des PPE corrompues ou malhonnêtes dans presque tous les pays.

Exemple 13 : Blanchiment d'argent obtenu dans le cadre d'une opération de corruption à grande échelle par un proche d'une PPE

Une cassette vidéo tournée dans un pays A montrait le conseiller de la Présidence, M. Z., offrant apparemment un pot-de-vin à un homme politique de l'opposition. La publicité faite autour de M. Z, généralement considéré comme l'éminence grise du Président alors en fonction dans le pays A, a conduit le Président à nommer un procureur spécial qui a lancé de nombreuses enquêtes dans le pays A sur les activités illégales de M. Z et de ses associés. Une enquête menée dans un pays B a amené les autorités de ce pays à geler une somme d'environ USD 48 millions appartenant à M. Z[6]. M. Z a fui le pays et a été finalement arrêté et extradé vers le pays A où il a dû répondre de plusieurs accusations : corruption, trafic de drogue, enrichissement illicite et autres.

Avant l'arrestation de M. Z, l'un de ses associés, M. Y, avait été arrêté en vertu d'un mandat d'arrêt assorti d'une demande d'extradition du pays A. M. Z et ses associés, dont M. Y, se procuraient les fonds confisqués dans cette affaire en abusant de la position officielle de M. Z en sa qualité de conseiller de l'ancien Président du pays A. Les principales manœuvres frauduleuses portaient sur l'achat de matériel militaire et de contrats de services ainsi que sur le placement à des fins criminelles de fonds de pension publics.

M. Y était ainsi impliqué dans un vaste système de commissions dans lequel des fonds étaient détournés du trésor et des fonds de retraite de l'armée et de la police du pays A. M. Y et ses complices ont utilisé l'argent des

[6] Un montant supplémentaire de USD 22 million a été ensuite découvert.

fonds de pension et leur propre argent pour acquérir une participation majoritaire dans une institution bancaire du pays C, la banque M, qui en juin 1999 a été rachetée par une autre banque du pays A. M. Y était chargé de trouver des placements pour le compte de la banque M et il a identifié dans ce cadre des projets de construction et des projets immobiliers que la banque et les fonds de pension devaient financer. Il contrôlait également les entreprises de bâtiment chargées de la construction des projets. M. Y a conçu un schéma consistant à majorer 25 pour cent le coût réel des projets d'investissement des fonds de pension qui était facturé à la banque M. Les projets recommandés par M. Y étaient automatiquement approuvés par le conseil d'administration du fonds de pension de la police, car plusieurs de ses membres percevaient des commissions. Un projet de USD 25 millions a ainsi été « gonflé » frauduleusement de USD 8 million. De la même façon, M. Y contrôlait secrètement plusieurs sociétés-écrans créées par lui, utilisées pour placer des prêts de la banque M en échange de commissions versées par les emprunteurs. En cas de défaillance des emprunteurs, M. Y rachetait les projets en faillite pour des sommes extrêmement modiques et les revendait avec un bénéfice.

En outre, M. Y et les membres du conseil d'administration de la banque M avaient été autorisés par le gouvernement du pays A à s'occuper de l'achat d'avions militaires pour le pays. En deux opérations seulement, le gouvernement du pays A avait acquitté un surcoût de USD 150 millions du fait d'une surfacturation frauduleuse de 30 pour cent. Cet argent illicite était censé transiter par l'intermédiaire de la banque M. De là, il était acheminé vers de nombreux comptes bancaires ouverts à différents noms dans des banques situées à l'étranger de manière à dissimiler l'origine des fonds.

M. Y utilisait toujours le même groupe de banques à l'étranger pour blanchir sa part des produits d'activités criminelles et celles des autres. Mme D, banquière mariée à un cousin de M. Y, ancienne membre du conseil d'administration de la banque N, a aidé celui-ci à dissimuler plus de USD 20 millions dans un seul pays.

M. Y a ouvert un compte bancaire dans le pays C sur lequel ont transité quelque USD 15 millions avant qu'il soit arrêté. Au départ, l'ouverture du compte n'avait pas soulevé de soupçons parce que des ressortissants du pays A ouvraient souvent des comptes dans le pays C pour protéger leurs avoirs de l'inflation. Toutefois, les institutions financières gérant les comptes bancaires et de courtage appartenant à M. Y, Mme D et d'autres ou contrôlés par eux ont progressivement noté une activité inhabituelle sur ces comptes. Selon des représentants de la banque, les opérations financières effectuées par M. Y n'avaient apparemment aucune justification commerciale et l'origine des fonds était suspecte.

78. Il apparaît par ailleurs que les PPE, étant donné le caractère souvent très visible de leur charge, dans leur pays et à l'étranger, ont très souvent recours à des intermédiaires qui effectuent des transactions financières pour leur compte. Il n'est donc pas inhabituel que des associés, proches ou parents d'une PPE réalisent des opérations ou, de toute autre manière, détiennent ou transfèrent des actifs en leur nom propre pour le compte de cette PPE. Le recours à des intermédiaires n'est pas forcément le signe en soi d'une activité illégale, dans la mesure où de tels intermédiaires sont également utilisés lorsque les affaires ou les biens d'une PPE sont tout à fait légitimes. Dans de nombreux cas cependant, le recours à des intermédiaires pour soustraire la PPE à attention des observateurs peut également faire obstacle au devoir de vigilance qui devrait être exercé vis-à-vis de chaque client. Les choses sont se compliquent encore lorsque la personne qui agit pour le compte de la PPE, voire la PPE elle-même, jouissent d'une forme ou d'une autre de statut particulier, leur conférant par exemple l'immunité diplomatique.

Exemple 14 : Un haut fonctionnaire de l'État blanchit de l'argent obtenu par détournement de fonds publics grâce à des membres de sa famille

La famille d'un ancien haut fonctionnaire du pays A ayant occupé différentes fonctions politiques et administratives a créé dans un pays B, centre financier offrant des conditions fiscales intéressantes, une fondation dont le principal bénéficiaire était le fils de ce fonctionnaire. La fondation a ouvert dans un pays C un compte à partir duquel un montant d'environ USD 1,5 million a été transféré sur un compte joint ouvert deux mois plus tôt auprès d'un établissement bancaire situé dans le pays D voisin. Ce virement a attiré l'attention de cette institution, qui a estimé légitime de faire une déclaration d'opération suspecte auprès de la cellule de renseignements financiers de son pays.

Les enquêtes menées à la suite de la déclaration d'opération suspecte ont permis de retrouver la trace, sur le même compte, de deux virements internationaux antérieurs portant sur des montants considérables originaires des comptes bancaires de l'épouse du fonctionnaire dans leur pays d'origine (A), et ont également révélé que l'épouse possédait des comptes dans d'autres établissements bancaires de ce pays, qui étaient également approvisionnés par des virements internationaux suivis de retraits. L'absence de toute justification économique apparente des opérations bancaires effectuées et les informations obtenues dans le cadre des poursuites pour détournement de fonds publics initiées à l'encontre du haut fonctionnaire dans son pays ont abouti à la présomption, dans cette affaire particulière, de l'existence d'un système conçu pour blanchir les produits dérivés de ces détournements. Le fonctionnaire concerné a été ensuite arrêté pour être interrogé et mis en examen alors qu'il s'apprêtait à fermer son compte en banque. Une enquête a été ouverte.

79. Outre le recours à des tiers, les PPE qui souhaitent transférer ou dissimuler des profits illégaux le font généralement en faisant transiter les fonds par des réseaux de sociétés-écrans ou de banques extraterritoriales dans des endroits situés hors de leur pays d'origine et qui ne sont pas susceptibles de divulguer des détails sur les transactions concernées. Dans d'autres cas, leurs opérations financières peuvent être camouflées derrière d'autres types de dispositifs juridiques opaques tels que des fiducies (*trusts*). Là encore, les possibilités, pour une institution financière, d'exercer intégralement son devoir de vigilance et d'appliquer les principes de connaissance de la clientèle aux PPE dans de tels cas sont singulièrement amoindries.

Exemple 15 : Implication d'un cadre d'une entreprise publique dans une opération de corruption à haut niveau

Une enquête concernant M. A, haut fonctionnaire salarié d'une entreprise publique A, a montré qu'il recevait des paiements excessifs sur un certain nombre de comptes qu'il possédait et exploitait. M. A, en sa qualité de vice-président de la société A, percevait un revenu annuel de plus de USD 200 000. L'enquête a montré que M. A possédait dans différents pays 15 comptes bancaires sur lesquels plus de USD 200 millions avaient transité. M. A utilisait l'argent placé sur ces comptes pour étendre son influence politique et obtenir de gouvernements étrangers des contrats de grande ampleur pour le compte de la société A.

L'enquête a par ailleurs montré qu'un compte en fiducie avait été créé pour servir de canal par lequel les paiements émanant de la société A étaient ensuite acheminés sur un certain nombre de petits comptes contrôlés par M. A. Celui-ci procédait ensuite à des virements, ou à des retraits d'espèces. Les fonds ainsi retirés étaient utilisés pour verser des pots-de-vin, parmi les bénéficiaires desquels figurent des chefs d'État et de gouvernement, de hauts fonctionnaires, des dirigeants d'entreprises publiques ou encore des hommes politiques importants de plusieurs pays, ainsi que des parents et de proches associés de M. A.

Une enquête plus approfondie portant sur les opérations financières effectuées sur les comptes de M. A a montré qu'une société-écran était utilisée pour effectuer et recevoir des paiements. En plus de cette activité régulière, des dépôts en espèces étaient effectués de manière irrégulière (souvent plus d'un par jour), ainsi que des retraits d'un montant anormalement élevés. Plus de USD 35 millions ont ainsi été retirés en espèces d'un seul compte en six semaines. De tels mouvements étaient incohérents par rapport à l'activité précédente du compte. Les enquêteurs ont noté également un fractionnement délibéré des dépôts en petites sommes, ce qui montre que M. A connaissait les obligations de déclaration et tentait ainsi de s'y soustraire. Parmi les bénéficiaires de paiements effectués par M. A, en espèces ou par virements, on trouvait plusieurs PPE ainsi que des personnes qui leur étaient associées.

<u>Homme politique, haut fonctionnaire</u>

Un intermédiaire a reçu de la société A un montant de USD 50 millions. Cet intermédiaire a ensuite transféré l'argent sur deux comptes extraterritoriaux ; les fonds ont ensuite été déposés sur des comptes de société également extraterritoriaux. On a découvert que les propriétaires effectifs de ces comptes étaient un ancien chef des services secrets d'un pays B et un secrétaire d'État à la défense d'un pays C.

Épouse d'une PPE

De l'argent a été viré par la société A sur l'un des comptes bancaires de M. A, lequel a ensuite placé les fonds sur le compte-client d'un avocat puis sur un compte bancaire extraterritorial. La propriétaire effective de ce compte extraterritorial était l'épouse récemment divorcée d'une PPE, Mme C. Ce compte a été approvisionné par des fonds utilisés pour acquérir une propriété estimée à plus de USD 500 000 et une voiture, redécorer l'appartement de Mme C et lui verser une allocation mensuelle de USD 20 000.

Ami et associé d'une PPE

La société A a versé de l'argent sur un compte bancaire dans le pays D. La banque du pays D a eu ensuite pour instruction de transférer l'argent à un associé de M. A, qui détenait un compte dans le même établissement. Cet associé a ensuite « prêté » un montant équivalent à une PPE.

80. Selon l'un des membres du GAFI, il existe deux méthodes principales pour détecter les activités financières illégales d'une PPE. La première, c'est lorsqu'il y a un changement de gouvernement dans le pays et que les activités illégales d'une PPE sont mises au jour par ceux qui lui succèdent. Cette méthode, si elle est la plus évidente, n'est toutefois pas complètement fiable. En effet, dans certains cas, les accusations de pratiques illégales ou de corruption formulées par la nouvelle équipe ne sont qu'une manœuvre politique. La deuxième manière de détecter les opérations financières illégales d'une PPE consiste à repérer des transactions suspectes ou inhabituelles dans laquelle des personnes agissant pour son compte peuvent être impliquées. Lorsque de telles transactions sont replacées dans le contexte de la relation entre un intermédiaire et une PPE pour le compte de laquelle celui-ci agirait, on peut alors avoir davantage de motif de soupçonner que les fonds ou les actifs concernés ont une origine illégale.

81. En plus des éléments cités ci-dessus qui constituent des obstacles potentiels à l'exécution du devoir de vigilance vis-à-vis des PPE, à l'application des principes de connaissance de la clientèle ou à la détection des liens existant entre les PPE (ou ceux qui leur sont associés) et une activité criminelle, il arrive quelquefois que des enquêtes portant sur des soupçons de connexions financières illicites soient entravées par des caractéristiques propres aux PPE. La plus importante, s'il faut en croire l'un des experts participant à la réunion, est l'absence du « soutien politique » nécessaire, en particulier lorsqu'il apparaît que l'enquête risque de mettre au jour des connexions entre une PPE étrangère et de hauts fonctionnaires du pays dans lequel l'enquête a lieu. A l'évidence, l'impossibilité d'obtenir les informations nécessaires de la part d'homologues étrangers, ou du moins de les obtenir en temps opportun, empêche également de mener de telles enquêtes à leur terme.

Exemple 16 : Blanchiment des produits de détournements de fonds

Les comptes bancaires du ministre du pétrole (M. Y) d'une ancienne dictature sous laquelle de nombreux détournements avaient été commis ont été crédités d'un montant de USD 6 millions en l'espace de quelques mois. Ceci est apparu comme un motif suffisant pour que l'affaire soit portée devant les autorités judiciaires qui ont décidé de mettre le ministre en accusation.

Au cours de son enquête, la cellule de renseignements financiers a découvert que M. Y agissait sous un faux nom. Un compte récemment ouvert, appartenant à M. Y, avait été crédit d'un chèque de notaire d'un montant de plus de USD 575 000 au titre de la vente d'une propriété. Or, cette somme ne correspondait en rien à la valeur marchande de ce bien.

Conséquences au plan de l'action publique

82. L'examen de la question des PPE au cours de l'exercice de cette année sur les typologies a plusieurs implications sur les mesures de lutte contre le blanchiment et le financement du terrorisme. Les experts ont été plusieurs à souligner que d'un certain point de vue, le problème des activités financières des PPE est le même que celui des activités de n'importe quel client d'une institution

financière : le devoir de vigilance doit s'exercer, que ce soit vis-à-vis de la PPE ou des personnes qui agissent pour son compte. De la même façon, les principes de connaissance de la clientèle doivent leur être appliqués sans exception.

83. Lorsqu'on est en présence de personnes qui agissent ou qui semblent agir pour le compte de quelqu'un d'autre, que ce soit pour réaliser des opérations financières ou détenir des actifs, il est impératif de déterminer quel est le bénéficiaire effectif/propriétaire réel ou final. Une délégation a indiqué qu'il était difficile, une fois le propriétaire réel identifié, de savoir si cette personne était bien une PPE dans son pays d'origine. Les participants ont souligné que les responsables politiques changeaient, même dans un seul et même pays, si bien qu'une personne qui est à un moment donné une PPE risque de ne plus l'être dans le gouvernement suivant. Deux solutions possibles ont été citées : l'une consisterait à constituer une base de données contenant des informations sur les hauts fonctionnaires et membres de gouvernement en fonction. Cette solution semble idéale, mais certaines délégations ont attiré l'attention sur les difficultés qu'il y aurait à tenir une telle base de données. L'autre solution consisterait simplement à constituer des bases de données appropriées dans chaque pays et à encourager encore davantage la coopération informelle (entre cellules de renseignements financiers par exemple) lors d'enquêtes sur d'éventuelles PPE et sur leurs relations financières.

84. Les experts du GAFI ont conclu que les techniques utilisées par les PPE pour blanchir les produits perçus de manière illicite étaient très proches de celles mises en œuvre par tout autre blanchisseur criminel. Considérées du seul point de vue des institutions financières, elles ont l'air rigoureusement identiques. Il a été souligné au cours d'exercices antérieurs que les PPE ont parfois recours à des schémas bancaires spécifiques qui leur permettent de créer les réseaux complexes dont ils ont besoin pour protéger les actifs illicites qu'ils ont réussi à se procurer. Là encore, les participants ont réitéré qu'il s'agissait d'une autre raison importante pour que les institutions financières exercent pleinement leur devoir de vigilance vis-à-vis des PPE, et s'acquittent notamment de leur obligation de déclarer leurs soupçons de blanchiment.

85. Enfin, s'il est entendu que la question des PPE ne concerne par définition que les « personnes exposées » de haut niveau et les personnes qui leur sont associées, les experts ont estimé que la question de la corruption à des niveaux inférieurs était également importante. Pour reprendre les mots d'une délégation, le « plus gros risque » pour le système financier dans certains pays ou territoires « est la corruption endémique » et, en particulier, le fait que les hauts fonctionnaires occupant des postes à responsabilité soient sous-payés. Les experts ont estimé que cette question devrait être abordée de manière systématique, dans une perspective mondiale prenant en compte la diversité de nature et d'ampleur de la corruption dans les pays développés et dans les pays en développement.

V. LES OUVREURS DE PORTE (OU « GATEKEEPERS ») ET LE BLANCHIMENT DE CAPITAUX

86. Au fur et à mesure que les dispositifs de lutte contre le blanchiment sont appliqués dans les institutions financières, le risque d'être découvert augmente pour ceux qui cherchent à utiliser le système bancaire afin de blanchir les produits de leurs activités criminelles. De plus en plus, les blanchisseurs recherchent les conseils ou les services de professionnels spécialisés afin de faciliter leurs opérations financières. Cette tendance à l'implication de différents spécialistes des questions juridiques ou financières, ou « ouvreurs de porte » ou « gatekeepers », dans les montage de blanchiment, a déjà été observée par le GAFI[7] et reste une réalité aujourd'hui. La version révisée des Quarante recommandations du GAFI, publiée en juin 2003, aborde ce problème et appelle au renforcement des mesures financières préventives vis-à-vis des professions juridiques et financières qui courent le risque d'être impliquées dans des opérations de blanchiment.[8] Pour toutes ces raisons, le GAFI a décidé de se pencher une fois encore sur la manière dont les services de ces professionnels pourraient être détournés à des fins de blanchiment.

87. Les avocats, notaires, comptables et autres professionnels exercent un certain nombre de fonctions importantes lorsqu'il s'agit d'aider leurs clients à organiser et à gérer leurs affaires financières. En premier lieu, ils dispensent des conseils aux personnes physiques et aux entreprises sur des questions aussi diverses que les placements, la création de sociétés, les fiducies (*trusts)* et autres constructions juridiques, ou encore l'optimisation de la situation fiscale. En outre, les juristes préparent et, le cas échéant, remplissent eux-mêmes les papiers nécessaires à la création de structures de sociétés ou d'autres constructions juridiques. Enfin, certains de ces professionnels s'occupent parfois directement d'exécuter certains types de transactions financières (détention ou versement de fonds relatifs à l'acquisition ou à la vente d'un bien immobilier par exemple) pour le compte de leurs clients.

88. Toutes ces fonctions parfaitement légitimes peuvent également être recherchées par des groupes relevant de la criminalité organisée, ou par des criminels individuels. Ils le font parfois pour des raisons purement économiques ; toutefois, le désir de profiter du savoir-faire de ces professionnels pour mettre sur pied des mécanismes qui permettront de blanchir des produits d'origine criminelle joue un rôle plus important encore. Ce savoir-faire recouvre aussi bien des conseils prodigués en ce qui concerne les structures de sociétés et les localisations extraterritoriales les mieux adaptées à l'opération souhaitée que la constitution effective des sociétés ou des fiducies (*trusts)* qui en forment le cadre. Les ouvreurs de porte sont quelquefois aussi sollicités pour donner une apparence de légitimité à ces opérations en servant en quelque sorte d'intermédiaires dans les relations avec les institutions financières. Sur la base des documents examinés cette année, les experts semblent confirmer les conclusions de travaux antérieurs du GAFI sur les typologies.

Exemple 17 : Un comptable et des avocats prêtent la main à une opération de blanchiment

Des mouvements suspects portant sur plus de USD 2 millions ont été repérés : l'argent était envoyé par petits montants par différentes personnes qui donnaient des ordres de virement et d'effets bancaires pour le compte d'un cartel de trafiquants de drogue qui devait importer 24 kg d'héroïne dissimulés dans du fret à destination d'un pays Z. Les effets bancaires acquis auprès de différentes institutions financières du pays Y (pays d'origine de la drogue) étaient ensuite utilisés pour acheter des biens immobiliers dans le pays Z.

[7] Voir à ce propos des rapports antérieurs sur les typologies : FATF-IX: http://www.fatf-gafi.org/pdf/TY1998_fr.pdf, FATF-XI: http://www.fatf-gafi.org/pdf/TY2000_fr.pdf et FATF-XII: http://www.fatf-gafi.org/pdf/TY2001_fr.pdf

[8] La Recommandation 12 prescrit désormais d'étendre le devoir de vigilance et les obligations de conservation des documents aux avocats, notaires, autres professions juridiques indépendantes et comptables. La Recommandation 16 impose à cette catégorie de professions l'obligation de déclarer les opérations suspectes, sous réserve du respect du secret professionnel ou du privilège légal.

Le cartel avait recours aux services d'un comptable pour ouvrir les comptes en banque et faire enregistrer les sociétés. Ce comptable donnait également des conseils en placement aux dirigeants du cartel.

Le cartel faisait également appel à un cabinet d'avocats pour acquérir les biens immobiliers grâce aux effets bancaires rachetés à l'étranger une fois qu'ils avaient d'abord transité par le compte en fiducie des avocats. Ceux-ci avaient également créé des fiducies (*trusts)* et des sociétés familiales.

Exemple 18 : Des juristes professionnels participent à une opération de blanchiment

Un administrateur siégeant au conseil de plusieurs entreprises industrielles a détourné plusieurs millions de dollars en utilisant les comptes bancaires de sociétés extraterritoriales. Une partie des fonds détournés étaient ensuite investis dans l'immobilier dans un pays Y grâce à des sociétés civiles de placement immobilier gérées par des associés de la personne coupable de l'infraction principale.

L'enquête ouverte dans le pays Y à la suite d'une déclaration de la cellule de renseignements financiers a permis d'établir que la mise sur pied et le fonctionnement de ce schéma de blanchiment d'argent avaient été facilités par des comptables et des juristes, en d'autres termes des ouvreurs de porte. Ces ouvreurs de porte avaient aidé à arranger un certain nombre de prêts et à mettre en place les différents mécanismes juridiques, en particulier en constituant les sociétés civiles de placement immobilier utilisées pour acquérir les biens. Ces professionnels prenaient également part à la gestion des structures constituées dans le pays Y. L'enquête est encore en cours.

Exemple 19 : Un comptable prodigue des conseils financiers spécialisés à des représentants de la criminalité organisée

Une action menée par des autorités opérationnelles a permis de découvrir l'existence d'un comptable, M. J , soupçonné de faire partie de l'organisation criminelle de blanchiment et de réinvestissement des produits illicites tirés du trafic de drogue dirigée par M. X. Le rôle joué par M. J était principalement celui d'un « consultant juridique et financier ». Il avait pour mission d'étudier les aspects techniques et juridiques des placements prévus pour l'organisation et d'identifier les techniques financières les plus appropriées pour que ces investissements semblent licites du point de vue fiscal. Il devait également s'efforcer dans la mesure du possible de rendre ces placements rentables. M. J était un spécialiste des procédures bancaires et des instruments financiers internationaux les plus complexes. En fait, c'est lui le véritable « cerveau » financier du réseau chargé de réinvestir les fonds à la disposition de M. X. M. J opérait en « saupoudrant » les transactions financières entre différentes zones géographiques, grâce à des opérations triangulaires entre sociétés et entre institutions de crédit étrangères, en procédant à des virements électroniques et en utilisant des lettres de crédit stand-by données en garantie de contrats commerciaux, les fonds étant ensuite investis dans d'autres activités commerciales.

89. Un certain nombre de membres du GAFI ont commencé à se pencher de plus près sur le rôle joué par les ouvreurs de portes pour faciliter le blanchiment. Dans un pays qui a étendu l'obligation de déclaration d'opérations suspectes aux professions libérales juridiques et financières, on s'est rendu compte que moins de deux pour cent des rapports faisant état de l'implication d'avocats ou de notaires émanait de ces professions elles-mêmes. Ainsi, dans la majorité des cas, ce sont les institutions financières qui ont détecté les activités potentiellement suspectes. Et parmi ces rapports, quelque 40 pour cent concernaient l'ouverture ou la gestion de « comptes en fiducies ». Parmi les opérations considérées comme suspectes, on peut citer la succession rapide de dépôts ou de retraits en espèces sur un compte, des retraits ou virements de fonds provenant de sources inconnues ou de sources n'ayant apparemment aucun lien explicable, ou encore des opérations portant sur des montant paraissant incompatibles avec leur objet économique déclaré.

Exemple 20 : Un avocat utilise des sociétés extraterritoriales et des comptes en fiducie pour blanchir des capitaux

M. S était à la tête d'une organisation qui importait dans un pays A des stupéfiants en provenance d'un pays B. Il employait un avocat pour blanchir les produits dérivés de ces activités.

Afin de blanchir les capitaux générés par l'importation des stupéfiants, l'avocat a mis sur pied un réseau de sociétés extraterritoriales. Ces entités étaient enregistrées dans un pays C, où le contrôle des propriétaires effectifs, des livres comptables et de la situation financière était très vague. Une société de gestion locale située dans un pays D administrait ces sociétés. Toutes ces entités servaient à camoufler les mouvements de fonds illicites, l'acquisition d'actifs et le financement d'activités criminelles. M. S était propriétaire de 100 pour cent du capital au porteur de ces entités extraterritoriales.

Dans le pays A, un groupe de personnes et de sociétés n'ayant apparemment aucun lien avec M. S transférait des sommes considérables dans le pays D, où l'argent était déposé sur le compte des sociétés extraterritoriales de M. S, ou transitaient par ceux-ci. Il est apparu que ce même réseau avait été utilisé pour transférer d'importantes sommes à une personne dans un pays E, laquelle s'est révélée ensuite être responsable des expéditions de drogue à destination du pays A.

Plusieurs autres avocats étaient utilisés, par le biais de leurs comptes en fiducie qui servaient à recevoir des espèces et à transférer des fonds, officiellement pour le bénéfice de clients situés dans le pays A. Approchés par les autorités opérationnelles dans le cadre de l'enquête, plusieurs de ces avocats ont mis en avant le « secret professionnel » pour justifier leur refus de coopérer. Parallèlement, l'avocat avait constitué un réseau similaire distinct (qui reposait notamment sur les comptes en fiducie d'autres avocats) afin d'acquérir des actifs et de placer des fonds dans des structures et instruments destinés à masquer l'identité de leur bénéficiaire effectif. L'avocat n'a été accusé d'aucune infraction pénale dans le pays A. Les enquêteurs soutiennent toutefois que ses liens avec M. S et les opérations effectuées pour le compte de celui-ci sont pourtant irréfutables.

Exemple 21: Un avocat utilise le compte d'un client pour faciliter une opération de blanchiment

Sur une période de trois ans, M. X a rapatrié des fonds dans un pays Y pour son usage et à son profit. Il était assisté en cela par des avocats et des comptables ayant recours à de fausses transactions et à des sociétés extraterritoriales. M. Y, un ancien avocat, a aidé M. X dans ses opérations de rapatriement en gérant la société et les comptes bancaires extraterritoriaux de M. X dans plusieurs centres financiers importants. M. Y rédigeait des documents censés être des accords de « prêt » entre la société-écran extraterritoriale et un prête-nom de M. X dans un pays Y. Ces accords de prêt servaient à justifier le transfert de plusieurs millions issus de comptes bancaires situés dans plusieurs pays différents à destination du pays d'origine de M. X. A leur arrivée sur les comptes bancaires ouverts par le prête-nom de M. X, les fonds étaient transférés à ce dernier. L'avocat de M. Y utilisait les comptes bancaires du cabinet juridique pour faciliter les transferts.

90. Un autre pays membre du GAFI a indiqué que des groupes de criminalité organisée arrivaient à se protéger encore plus de toute détection en utilisant un ou plusieurs ouvreurs de porte « corrompus » pour faire transiter des fonds par des structures constituées à l'origine par une autre équipe d'ouvreurs de porte. De cette manière, les ouvreurs de porte appartenant à ce « deuxième niveau » n'ont pas besoin d'être impliqué dans le montage, et le risque pour leurs auteurs est encore réduit grâce à une séparation supplémentaire par rapport à la procédure de blanchiment. Selon ce pays, deux méthodes de recours à des ouvreurs de porte sont privilégiées : les transactions immobilières et l'utilisation de spécialistes du droit et de la comptabilité pour constituer des pistes d'audit parfaitement opaques. Dans le premier cas, les procédés utilisés sont le transfert ou la procédure translative de propriété, parce qu'il est ainsi possible de blanchir efficacement des montants importants en une seule transaction. Cette délégation a également fait remarquer que souvent, les comptables chargés de brouiller la piste de vérification pour une opération de blanchiment n'étaient souvent même pas connus des enquêteurs, parce qu'en fait, ils ne participent directement à aucune des opérations financières concernées.

Exemple 22 : Utilisation d'un fonds en fiducie pour recevoir de l'argent sale et acquérir des biens immobiliers

Un avocat avait été chargé par un de ses clients, trafiquant de drogue, de déposer des espèces sur son compte en fiducie puis d'effectuer des paiements réguliers au titre d'hypothèques sur des propriétés dont le trafiquant

était le propriétaire effectif. L'avocat a perçu des commissions sur la vente de ces propriétés et la négociation des hypothèques. S'il a reconnu avoir reçu des sommes en espèces du trafiquant, les avoir déposées sur son compte en fiducie et avoir géré les paiements au titre des hypothèques contractées, il a nié avoir eu connaissance de l'origine des fonds.

Conséquences au plan de l'action publique

91. De nombreux experts ont signalé que même lorsque l'obligation de déclaration d'opérations suspectes s'applique déjà aux ouvreurs de porte, le nombre de déclarations est souvent faible. Si, dans certains pays, cette faiblesse peut être attribuée au caractère relativement récent de la mise en œuvre de telles règles, il n'en reste pas moins que certains éléments sont encore perçus comme des obstacles à une participation pleine et entière des ouvreurs de porte à la lutte contre le blanchiment de capitaux. Ceci est sans doute dû en grande partie au manque de prise de conscience de la part des professions concernées, ou à des hésitations qui peuvent être mises sur le compte de la tradition de secret professionnel. Une délégation a toutefois souligné que les ouvreurs de porte avaient accès à des informations qui peuvent se révéler fondamentales pour comprendre certains montages complexes de blanchiment, et leur contribution serait donc indispensable à la détection de ces montages. Il est en conséquence important que les professions juridiques et comptables qui rendent des services financiers ou dispensent des conseils en la matière disposent d'un cadre juridique clair leur permettant de déclarer toute opération suspecte.

92. Il est également évident que tant les ouvreurs de porte que les institutions financières à laquelle ils ont à faire doivent exercer pleinement leur devoir de vigilance et mettre en œuvre toutes les procédures de vérification de leur clientèle. Selon toute probabilité, le nombre de juristes et de professionnels de la finance oeuvrant sciemment à faciliter des opérations de blanchiment est relativement faible. Toutefois, comme l'ont indiqué plusieurs experts participant à cet exercice sur les typologies, si les organisations criminelles cherchent à s'adjoindre les services des ouvreurs de porte, c'est principalement pour donner une apparence de légitimité à leurs opérations financières.

CONCLUSION

93. Ainsi que cela a été mentionné au début du présent rapport, l'exercice de cette année sur les typologies avait pour objectif d'examiner des questions ayant une acuité particulière pour les travaux actuels du GAFI, et de revenir sur des méthodes et tendances initialement identifiées lors de travaux antérieurs sur les typologies. Le financement du terrorisme et la mise en œuvre des Huit Recommandations Spéciales reste une préoccupation de fond du GAFI, c'est pourquoi l'examen du rôle des virements et des organisations à but non lucratif dans le financement du terrorisme inscrit cette année à l'ordre du jour de l'exercice sur les typologies a été considéré comme essentiel aux missions globales du GAFI. L'étude de la vulnérabilité du secteur des assurances au regard du blanchiment de capitaux a permis de revenir, en les approfondissant, sur certains points relevés au cours de l'exercice de l'année dernière. Enfin, si les questions relatives aux PPE et aux ouvreurs de porte avaient déjà été abordées au cours d'exercices précédents, leur inclusion dans le programme de cette année se justifie par la publication de la version révisée des Quarante Recommandations, qui contient un certain nombre de mesures répondant spécifiquement aux risques propres à ces deux domaines.

94. Une nouvelle approche a été utilisée pour préparer cet exercice et examiner trois des thèmes retenus cette année, à savoir les virements électroniques, les organisations à but non lucratif et le secteur des assurances. Cette nouvelle approche a permis d'étoffer l'analyse et la discussion de ces thèmes avant la réunion plénière des experts. La réunion elle-même a été ponctuée par des ateliers qui ont permis aux participants de mieux centrer les débats sur les thèmes retenus et ont constitué un vecteur supplémentaire d'échange de vues sur ces questions. Les experts ont pour la plupart réagi de manière positive à ces aménagements et il est en conséquence probable que les organisateurs tireront profit de cette expérience pour améliorer encore le déroulement des exercices futurs sur les typologies.

95. En ce qui concerne les virements électroniques et leurs liens avec le financement du terrorisme, les experts ont conclu que cette méthode était fréquemment utilisée pour alimenter diverses catégories d'organisations terroristes. Si les enquêteurs sont arrivés à reconstituer des pistes terroristes grâce à l'utilisation de virements une fois que cet usage avait été repéré, le fait que de nombreux virements transfrontaliers ne soient pas assortis d'informations complètes permettant d'identifier les donneurs d'ordre constitue un obstacle majeur à l'identification des liens avec le terrorisme. En outre, la détection initiale de l'utilisation des virements à des fins terroristes reste pour l'instant difficile étant donné le montant généralement modeste des transactions individuelles et l'absence générale d'autres indicateurs utiles.

96. Les organismes à but non lucratif et le rôle qu'ils peuvent jouer pour faciliter le financement du terrorisme continuent à préoccuper fortement le GAFI. Les experts réunis cette année pour l'exercice sur les typologies ont progressé dans leur compréhension des différentes manières permettant de détourner les OBNL de leur objet, ainsi que des « signaux d'alerte » financiers spécifiques qui peuvent signaler l'existence de tels détournements. Ils ont également tenté de cerner certaines questions concernant les systèmes de surveillance dans ce secteur et les mesures qui pourraient être prises pour rendre les OBNL moins vulnérables à un détournement potentiel par des terroristes. Des travaux devront encore être menés pour affiner la compréhension du phénomène des risques de financement du terrorisme concernant certaines parties spécifiques du secteur des OBNL dans certains pays.

97. Cette année, le GAFI s'est par ailleurs penché pour la première fois sur les risques spécifiquement associés au blanchiment dans le secteur des assurances. Les experts ont débattu pour savoir si le montant des opérations de blanchiment détectées dans ce secteur était disproportionnellement faible compte tenu de la taille du secteur dans son ensemble. Par ailleurs, il semble que certaines vulnérabilités potentielles soient inhérentes à la nature-même du secteur. Toutefois, les experts ne sont pas parvenus à un consensus sur ces questions. Il semble qu'on s'achemine vers une meilleure compréhension des vulnérabilités propres à des branches d'activités ou types de produits spécifiques ; cependant, les experts sont tombés d'accord sur le fait qu'il fallait poursuivre les travaux pour s'assurer que tous les domaines de risque étaient identifiés. De la même

façon, il sera sans doute nécessaire d'œuvrer à la mise au point d'indicateurs supplémentaires spécifiquement liés à ces domaines.

98. Au cours d'exercices antérieurs sur les typologies, le GAFI s'était penché sur certains risques de blanchiment associés aux personnes politiquement exposées. Les discussions qui ont suivi les exposés et la présentation des documents fournis pour l'exercice de cette année sur la question confirme des observations précédentes sur la nature et les tendances associés à ce risque. Si, dans certaines affaires, on a pu constater que les PPE avaient eu recours à des intermédiaires ou autres agents pour éviter d'être découverts, il apparaît très souvent que les activités financières illégales des PPE auraient pu être décelées si les institutions financières ayant ouvert ou gérant leurs comptes s'étaient correctement acquittées de leur devoir de vigilance. Les experts ont attiré l'attention sur certaines difficultés rencontrées pour déterminer si une personne doit être considérée comme une PPE et à ce jour, la meilleure solution semble résider dans un renforcement de la coopération informelle entre autorités homologues au niveau international.

99. Par ailleurs, le GAFI a examiné certains risques associés aux services rendus par les spécialistes du droit et de la finance, les « ouvreurs de porte ». Là encore, les travaux ont confirmé, en l'étayant quelque peu, la perception que l'on a des caractéristiques propres à ce secteur et qui le rendent vulnérables au blanchiment. De nombreux membres du GAFI ont commencé à faire appliquer des mesures ayant pour objet de soumettre les « ouvreurs de porte » aux mêmes obligations que celles que doivent actuellement respecter les institutions financières en matière de vérification de l'identité des clients, de conservation des documents et de déclaration d'opérations suspectes. Un certain nombre d'experts ont souligné que certains risques ou vulnérabilités constatés chez les « ouvreurs de porte » (de même que chez les PPE) pourraient être réduits si les mesures de lutte contre le blanchiment et contre le financement du terrorisme étaient appliquées de manière complète et cohérente.

100. Des pays issus de toutes les parties du monde, qu'ils soient ou non membres du GAFI, ainsi qu'un certain nombre d'organisations internationales, ont participé à l'exercice sur les typologies du GAFI-XV. Leurs experts ont su fédérer les expériences diverses glanées dans chaque pays lorsqu'il s'agit d'affronter les défis que représentent le blanchiment des capitaux et le financement du terrorisme pour les appliquer aux cinq thèmes retenus pour l'exercice de cette année. Une initiative telle que celle du GAFI sur les typologies sert évidemment à mieux connaître les domaines spécifiques sélectionnés, mais elle constitue également une source précieuse de confrontation des points de vue entre les spécialistes des autorités opérationnelles (police, autorités chargées des poursuites, autorités de réglementation, cellules de renseignements financiers) et ceux qui appartiennent aux cercles de décision politique. C'est cet échange de vues qui, en dernier ressort, constitue le cœur des efforts déployés par le GAFI pour promouvoir et, si nécessaire, affiner encore les Quarante Recommandations et les Huit Recommandations Spéciales sur le financement du terrorisme.