



**Onzième
Congrès des Nations Unies
pour la prévention du crime
et la justice pénale**

Bangkok, 18-25 avril 2005

Distr.: Générale
16 mars 2005

Français
Original: Anglais

Point 6 de l'ordre du jour provisoire*
**Criminalité économique et financière:
défis pour le développement durable**

**Atelier 5: Mesures de lutte contre la criminalité
économique, notamment le blanchiment d'argent****

Document d'information***

Table des matières

	<i>Paragraphes</i>	<i>Page</i>
I. Introduction	1-4	2
II. Usurpation d'identité	5-16	3
III. Blanchiment d'argent	17-36	7
A. Incrimination du blanchiment d'argent: cadre juridique	32-33	10
B. Enquêtes relatives aux infractions de blanchiment d'argent	34	10
C. Coopération internationale	35	11
D. Mesures de répression visant le produit du crime	36	11
IV. Assistance technique	37-47	11
V. Conclusions et recommandations	48-49	13
Annexe. Cas hypothétique à examiner lors de l'atelier 5		15

* A/CONF.203/1.

** La présentation du présent document d'information a été différée en raison de recherche et de consultations complémentaires.

*** Le Secrétaire général tient à exprimer ses remerciements à l'Institut pour la prévention du crime et le traitement des délinquants en Asie et en Extrême-Orient ainsi qu'au Gouvernement suédois pour l'aide qu'ils ont apportée à l'organisation de l'atelier 5.



I. Introduction

1. Parallèlement à la transformation des structures socioéconomiques, les progrès rapides qu'ont récemment connus les technologies de l'information et le secteur des transports ont favorisé la mondialisation, de par l'augmentation des transactions et la diversification des activités économiques, dont la nature est de plus en plus transnationale. Dans le sillage de ces changements, qui ont engendré de nouvelles possibilités de croissance et de développement, les préoccupations relatives à la criminalité économique ont également pris une dimension mondiale alors que le mode opératoire des groupes criminels est devenu plus sophistiqué et que l'ampleur de leurs activités s'est considérablement élargie. Cette tendance s'est accélérée avec la prolifération rapide des ordinateurs, la hausse considérable des utilisateurs de services sur Internet et l'expansion des économies fondées sur les cartes de crédit. De par leur nature même, les infractions commises au moyen d'Internet transcendent aisément les frontières nationales et se propagent dans le monde entier. Les criminels exploitent à fond Internet et le commerce électronique pour commettre des infractions économiques d'un pays à l'autre. La nature transnationale de ces infractions fait obstacle à leur détection et rend plus difficiles les enquêtes et les poursuites. Il est également devenu plus compliqué de localiser et de restituer le produit du crime. Par conséquent, la criminalité économique, dans une société en cours de mondialisation, représente un sérieux problème pour la communauté internationale et compromet le développement de l'économie mondiale.

2. Le onzième Congrès des Nations Unies pour la prévention du crime et la justice pénale donnera la possibilité de débattre de façon approfondie du vaste problème que représente la criminalité économique et financière. Dans l'optique de ces débats, le Secrétariat a établi un document de travail (A/CONF.203/7) qui soulève un certain nombre de questions à examiner et qui décrit de façon très détaillée les problèmes posés par cette forme de criminalité, notamment la conceptualisation de la criminalité économique et financière et les raisons pour lesquelles ces problèmes exigent de la communauté internationale une attention particulière.

3. L'atelier 5 offre aux représentants des gouvernements, aux experts et aux spécialistes une possibilité supplémentaire de mener un dialogue interactif axé sur l'étendue et l'impact de la criminalité économique dans ses multiples manifestations. L'examen de ce thème central sera également nécessaire pour formuler des recommandations pratiques et viables et pour déterminer les éléments nécessaires à une action nationale ainsi qu'à une coopération internationale, notamment en ce qui concerne l'assistance technique.

4. Plus particulièrement, l'atelier 5 pourrait servir de point de départ à l'examen des mesures de lutte contre la criminalité économique et le blanchiment d'argent, notamment pour débattre des questions suivantes:

a) Les tendances actuelles de la criminalité économique, notamment le blanchiment d'argent, en accordant une attention particulière à la typologie de cette criminalité;

b) La mesure dans laquelle les instruments juridiques internationaux existants, notamment la Convention des Nations Unies contre la criminalité transnationale organisée (résolution 55/25 de l'Assemblée générale, annexe I) et les

Protocoles s'y rapportant ainsi que la Convention des Nations Unies contre la corruption (résolution 58/4, annexe), pourraient être utilisés pour leur faire échec;

- c) La formulation de stratégies de prévention efficaces;
- d) Les nouvelles techniques d'enquête;
- e) La création de services de renseignement financier efficaces, et la question de l'optimisation de leur coopération entre eux;
- f) La coopération internationale et l'assistance technique.

Afin de tirer le meilleur parti de l'esprit pragmatique de l'atelier et d'encourager un dialogue interactif, un cas hypothétique destiné à être analysé et débattu figure en annexe du présent document d'information.

II. Usurpation d'identité

5. L'un des principes guidant les travaux du Programme des Nations Unies pour la prévention du crime et la justice pénale est la nécessité de faire en sorte que, face à tout accroissement des capacités des criminels, il soit répondu par un accroissement similaire des capacités des autorités chargées de la détection et de la répression et de la justice pénale. Un autre objectif du programme est de maîtriser la criminalité tant sur le plan national qu'international. L'examen des mesures prises aux plans national et international pour s'attaquer à l'usurpation d'identité s'inscrit dans la logique de ces deux objectifs.

6. On peut considérer que l'usurpation d'identité implique deux composantes distinctes et parallèles. La première est la phase préparatoire consistant à acquérir, rassembler et transférer des informations personnelles, que celles-ci soient immatérielles (par exemple, des informations virtuelles sur l'écran d'un ordinateur) ou matérielles (informations personnelles recopiées sur une feuille de papier à partir de l'écran d'un ordinateur ou d'un document concret). Il n'y a à cette étape aucune utilisation des informations pour tenter de commettre, ou pour commettre effectivement, une infraction pénale telle que la fraude, le vol ou l'usurpation de l'identité d'une autre personne. Les informations personnelles sont acquises pour être utilisées par la suite comme l'instrument d'une infraction. La deuxième composante de l'usurpation d'identité implique l'utilisation effective des informations personnelles pour tenter de commettre ou pour commettre une infraction pénale. Les informations personnelles sont alors utilisées soit pour acquérir une identité tout à fait nouvelle à tous égards (A se fait passer pour B), soit pour convaincre une victime qu'un aspect d'une transaction correspond à une chose qu'il n'est pas en réalité (par exemple, le solde d'un compte bancaire est de X dollars plutôt que de Y dollars en raison du fait que le compte appartient à B et non pas à A, qui se fait passer pour B).

7. L'usurpation d'identité implique donc une ou plusieurs actions s'inscrivant dans la continuité et qui vont finalement mener à commettre une infraction, généralement de nature économique. Dans la plupart des États, si une personne ne commet pas une infraction pénale (un vol par exemple) pour obtenir des informations personnelles, l'acquisition et la possession d'informations personnelles ne constituent pas en soi une infraction. Toutefois, de plus en plus d'éléments

indiquent que l'usurpation d'identité facilite la commission d'infractions économiques, tant au niveau national qu'international.

8. Dans de nombreux, sinon dans la plupart des États, la responsabilité pénale est souvent engagée uniquement après que le délinquant a effectivement utilisé les informations personnelles et non au moment où il les a acquises avec l'intention de les utiliser à des fins délictueuses. Par exemple, un délinquant peut obtenir sournoisement des informations relatives à une personne afin d'endosser l'identité de la victime et de commettre des fraudes, d'éviter d'être arrêté ou localisé ou, dans certains cas, de commettre des infractions liées à la criminalité organisée ou au terrorisme. Dans de nombreux États, à moins qu'une conspiration ou que des activités criminelles organisées puissent être prouvées, un ou plusieurs des actes suivants ne peuvent être incriminés: collecte, acquisition, conservation, possession, achat, vente, importation et exportation d'informations immatérielles relatives à une personne (c'est-à-dire des informations personnelles disponibles sur un ordinateur ou des listes écrites d'informations relatives à des personnes recopiées à partir de documents d'identité.)

9. Les moyens par lesquels les délinquants obtiennent ces informations personnelles peuvent être plus ou moins sophistiqués. Certaines de ces activités sont incriminées dans presque tous les pays (c'est le cas du vol) alors que d'autres ne le sont pas. Une liste des moyens les plus répandus pour obtenir des informations personnelles dans un but criminel est reproduite ci-dessous:

a) Vol de porte-monnaie et de portefeuilles, vol de courrier; réacheminement du courrier de la victime à l'adresse du délinquant;

b) Récupération dans une corbeille de documents donnant des informations personnelles sur la victime, par exemple le numéro d'une carte ou d'un compte bancaires ("fouille de poubelles");

c) Copie non autorisée de données numérisées (par exemple, "dispositif de ramassage" ("skimming") qui copie les numéros des cartes bancaires; une caméra cachée pour enregistrer le code secret accompagne ces dispositifs);

d) Obtention d'informations personnelles relatives à une personne décédée afin d'endosser son identité;

e) Obtention des informations personnelles à partir de sources publiques (par exemple, le "shoulder surfing" ou l'observation qui implique le fait de regarder par-dessus l'épaule d'une personne en train de saisir son code secret lors de l'utilisation d'une carte bancaire);

f) Obtention sur Internet d'informations relatives au profil d'une personne dans le but d'utiliser ces informations pour effectuer des opérations au nom de l'intéressé et à son insu;

g) Utilisation d'Internet pour diriger des victimes sur un site Web ressemblant à celui d'une entreprise légitime. Sur le site Web en question, il est demandé à la victime de donner des informations personnelles. Ces informations sont recueillies par des délinquants qui les utiliseront par la suite pour commettre des fraudes ou d'autres formes d'infraction économique (cette activité est appelée "phishing", ou pêche aux données personnelles);

h) Immixtion dans de grandes bases de données (consistant par exemple, à s'introduire dans les bases de données d'ordinateurs privés ou publics afin d'obtenir des informations sur des personnes dans le but de produire de faux documents d'identité);

i) Utilisation d'informations personnelles fournies par des fonctionnaires ou des employés de société corrompus afin de contrefaire des documents (par exemple de faux permis de conduire) ou d'obtenir de faux documents d'identité avec la complicité de ces fonctionnaires ou employés.

10. L'une des difficultés que rencontrent un grand nombre d'États lorsqu'ils s'attaquent au problème de l'usurpation d'identité est que les informations personnelles ne correspondent généralement pas à la définition de "propriété". Traditionnellement, le vol suppose que la "chose" immatérielle ou matérielle volée puisse être définie comme une "propriété". Par ailleurs, pour que les éléments de l'infraction soient présents, les actes concernant la "chose" doivent impliquer que son propriétaire en est effectivement privé. Dans de nombreux États, la simple violation de la confidentialité des informations personnelles peut ne pas suffire à elle seule pour établir des éléments de fraude ou de vol. Ainsi, dans de nombreux États, si aucune infraction pénale n'est associée à l'obtention d'informations personnelles proprement dite, alors la simple copie de cette information ou le fait d'amener insidieusement quelqu'un à dévoiler cette information peut également ne pas constituer une infraction. La diffusion d'informations personnelles qui ne correspondent pas à la définition de "propriété" n'est également pas considérée comme une infraction pénale dans la plupart des États. De ce fait, les informations personnelles deviennent un instrument utilisé pour commettre une infraction, mais leur acquisition, possession et cession à d'autres parties ne constituent pas en soi, une infraction.

11. Outre les difficultés que posent dans de nombreux États la définition juridique du mot "propriété" ou le fait qu'il soit nécessaire qu'il y ait dépossession de la "chose" détournée, les progrès technologiques ont également modifié la façon de commettre des infractions économiques au moyen du détournement d'informations personnelles. Ainsi, avant l'invention de l'ordinateur et d'Internet, un cas de fraude typique pouvait impliquer le l'usurpation par un individu de l'identité d'une autre personne et son utilisation pour se faire passer pour cette personne afin de bénéficier d'un prêt ou d'emprunter de l'argent à une banque. Le prévenu était impliqué dans tous les aspects, tant physiques que mentaux, de l'infraction. Il y avait généralement un contact physique entre le délinquant et sa victime.

12. L'avènement des ordinateurs et d'Internet a facilité la commission d'infractions impliquant différents acteurs dans une succession d'activités criminelles. Leur identification est rendue difficile par l'anonymat que procure en général l'informatique. Cela encourage le recours à de multiples acteurs qui agissent soit de concert soit de façon indépendante les uns des autres, mais qui savent que les informations personnelles sont collectées et transférées à des fins délictueuses. Le problème rencontré par les services de détection et de répression est qu'aucun de ces acteurs ne commet, tout au long du processus, l'ensemble des actes qui débouchent finalement sur la commission d'une infraction économique traditionnelle. Chacun d'eux porte la responsabilité de l'une des composantes de cette activité qui, cumulées, débouchent sur une infraction telle que la fraude. Cette

méthode est employée par les groupes criminels organisés pour soustraire des individus à des poursuites pénales.

13. Voici un exemple d'infraction impliquant plusieurs acteurs: A copie des informations personnelles relatives à différents individus à partir d'un ordinateur. Puis il vend ces informations à B, le cas échéant en utilisant des technologies sophistiquées telles qu'Internet ou une méthode plus traditionnelle, consistant notamment à se faire remettre une somme d'argent en échange des informations en question. B peut agir en tant qu'intermédiaire et vendre les informations à C, qui va les utiliser pour produire de faux documents d'identité. C vend les faux documents d'identité à des clients se trouvant dans différents pays. Certains de ces clients utilisent ces faux documents d'identité pour commettre des fraudes à l'encontre de victimes se trouvant dans d'autres pays. Certains des clients revendent les faux documents d'identité à des groupes criminels organisés ou à des terroristes pour faciliter la commission d'autres infractions, comme le trafic de drogues, le blanchiment d'argent ou la contrebande. Au regard des lois de nombreux États relatives aux associations de malfaiteurs ou aux modes de participation à la commission d'une infraction, A et B n'ont commis aucune infraction, même si leurs activités font partie intégrante du processus qui a permis de fournir à C des informations nécessaires pour qu'il puisse produire de faux documents d'identité.

14. La plupart des États ne prévoient pas l'infraction d'"usurpation d'identité". Il est toutefois difficile de dire si, d'un point de vue statistique, les cas de fraude impliquant une usurpation d'identité sont inclus dans les statistiques concernant la fraude en général. Cela complique les tentatives visant à suivre la tendance internationale de la croissance des infractions impliquant le détournement d'informations personnelles. Il est à espérer que l'étude demandée par le Conseil économique et social dans sa résolution 2004/26 du 21 juillet 2004 permettra de mieux comprendre les tendances nationales et transnationales de la fraude ainsi que du détournement à des fins criminelles et de la falsification des documents d'identité.

15. Au Canada et aux États-Unis d'Amérique, de récentes statistiques sur les fraudes commises par l'usage impropre de renseignements personnels confirment la progression spectaculaire de ce type d'infractions. Le Centre d'appel antifraude du Canada a ainsi signalé 8 187 appels pour usurpation d'identité en 2002 et 13 359 en 2003, ce qui représente une augmentation considérable. Selon lui, les pertes engendrées par ce type d'infractions se seraient chiffrées à 11,8 millions de dollars canadiens en 2002 et 21,6 millions en 2003 (voir son site Internet, à l'adresse <http://www.phonebusters.com>). Ces quatre dernières années, la Commission fédérale du commerce des États-Unis a indiqué que l'usurpation d'identité était le premier des motifs pour lesquels les consommateurs disposaient des plaintes auprès d'elle. En septembre 2003, elle a publié les conclusions d'une enquête selon lesquelles 27,3 millions d'Américains avaient été victimes d'usurpation d'identité au cours des cinq années précédentes. Le coût supporté par les consommateurs et les entreprises en 2002 aurait été de 53 milliards de dollars¹. D'après une autre enquête que la Commission a réalisée en 2003, les 10 millions de personnes victimes d'usurpation d'identité cette même année auraient passé 300 millions d'heures à tenter de compenser leurs pertes financières, restaurer leur cote de solvabilité et rétablir leur réputation². Le Conseil canadien des bureaux d'éthique commerciale a

estimé à 2,5 milliards de dollars canadiens les pertes subies par les consommateurs et les entreprises du fait de l'usurpation d'identité en 2002³.

16. La libre circulation des informations, nerf de l'Internet et, par conséquent, du commerce électronique, offre aux malfaiteurs d'innombrables possibilités de détourner des renseignements personnels et de les utiliser pour commettre des infractions. La collecte et le transfert de renseignements personnels à l'insu des personnes concernées en vue d'en faire un usage délictueux sont susceptibles de nuire à la sécurité économique et nationale des États Membres.

III. Blanchiment d'argent

17. On entend généralement par "blanchiment d'argent" la transformation du produit du crime dans le but d'en dissimuler ou déguiser l'origine illicite. Les auteurs d'infractions cherchent à tirer de ces dernières, grâce au blanchiment, un profit financier dont ils pourront par la suite jouir ou se servir. Le blanchiment est donc une opération très importante pour la plupart d'entre eux, en particulier lorsqu'ils commettent des infractions financières en vue principalement d'en tirer un profit financier. Le blanchiment leur permet aussi de poursuivre leurs activités délictueuses ou de financer leurs organisations criminelles.

18. L'argent étant, dans la plupart des cas, blanchi en recourant de manière impropre ou frauduleuse aux systèmes financiers en place, l'intégrité de ces derniers et des établissements financiers s'en trouve gravement menacée. Les établissements financiers touchés par le blanchiment sont plus susceptibles d'être victimes d'autres infractions financières et sont donc pris dans un cercle vicieux. Dans les pays en développement, le blanchiment entrave ou freine le développement économique. Une grosse somme d'argent blanchi qui échappe à la supervision et à l'action des autorités financières nationales fausse les politiques monétaires et les systèmes de taxation nationaux.

19. La Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes de 1988⁴ a marqué la première étape de la lutte ininterrompue de l'ONU contre le blanchiment d'argent. Cette lutte a d'abord visé le blanchiment du produit des infractions liées aux drogues, mais il est progressivement apparu que le blanchiment du produit d'autres infractions graves menaçait tout autant la société et devait donc être traité de façon identique. C'est pourquoi, dans des instruments internationaux plus récents, les États parties sont engagés à punir le blanchiment du produit tiré de toutes les infractions ou des plus graves d'entre elles.

20. Les attentats terroristes perpétrés le 11 septembre 2001 aux États-Unis ont porté sur le devant de la scène les craintes suscitées par ce phénomène dans le monde, et la communauté internationale est rapidement convenue de s'employer activement à empêcher le financement du terrorisme et à y mettre fin. La détection et l'analyse des éventuelles activités de blanchiment d'argent et de financement du terrorisme ayant beaucoup en commun, il est logique que ce soient les grandes organisations ayant piloté la lutte contre le blanchiment qui s'attaquent aussi au financement du terrorisme. Le Conseil de sécurité a vite réagi en créant, par sa résolution 1373 (2001) du 28 septembre 2001, le Comité contre le terrorisme, et le Service de la prévention du terrorisme de l'Office des Nations Unies contre la

drogue et le crime (ONUDC) est un élément à part entière du mécanisme de lutte de l'ONU contre le terrorisme. Il convient toutefois de noter qu'avant même le 11 septembre 2001, l'urgence de la situation se faisant sentir, il avait été conclu, en 1999, la Convention internationale pour la répression du financement du terrorisme (résolution 54/109 de l'Assemblée générale, annexe), entrée en vigueur en 2002. Le Groupe d'action financière sur le blanchiment de capitaux a également étendu sa mission à la lutte contre le financement du terrorisme.

21. Les formes et techniques de blanchiment d'argent ne cessent d'évoluer. Il est généralement admis que les auteurs d'infractions ont le plus souvent un temps (ou plus) d'avance sur leurs adversaires, à savoir les autorités chargées des enquêtes, pour ce qui est de repérer les failles de la législation antiblanchiment du pays. Les autorités chargées des enquêtes et les autres autorités compétentes doivent donc impérativement être au courant des dernières méthodes apparues pour réprimer efficacement le blanchiment.

22. Compte tenu de ce que les économies où prédominent les opérations en espèces permettent aux auteurs d'infractions de virer de l'argent ou de changer la forme de leurs avoirs sans laisser aucune trace d'opération financière, les enquêteurs éprouvent de grandes difficultés à localiser les mouvements d'argent et à en établir la preuve. Même dans les pays dont les systèmes financiers sont les plus perfectionnés subsiste un pan d'économie monétaire destiné à répondre à des besoins particuliers. Dans nombre de pays en développement dont le secteur financier structuré n'est pas pleinement développé, l'économie monétaire est le système financier le plus utilisé et le plus fiable, et il n'est pas facile de le réglementer par quelque moyen que ce soit. La fréquente détention d'avoirs sous forme de bijoux ou de pierres précieuses pose un problème identique lorsqu'elle remplace l'utilisation de monnaie fiduciaire.

23. Les systèmes parallèles de transfert de fonds ou d'autres avoirs qui contournent les établissements financiers officiels peuvent eux aussi faire obstacle à la lutte contre le blanchiment d'argent. Beaucoup tirent leur crédibilité de communautés culturelles, ethniques ou religieuses et ne cherchent habituellement ni à identifier les clients, ni à garder une trace des opérations réalisées, comme le prévoient les normes internationales auxquelles sont soumis les établissements financiers. Dans certains États où seuls les établissements qui y sont autorisés ou qui sont enregistrés comme banques peuvent proposer des services de virement d'argent ou de transfert d'avoirs, les systèmes parallèles de transfert de fonds sont nécessairement illégaux et clandestins. Dans beaucoup d'autres, ils constituent des systèmes financiers licites qui fonctionnent depuis bien plus longtemps que les services bancaires modernes.

24. Le rôle et l'utilisation potentiellement frauduleuse d'entreprises et de professions non financières aux fins du blanchiment ont récemment attiré l'attention internationale du fait de la multiplication des affaires. Sont concernés les avocats, notaires et personnes exerçant d'autres professions juridiques à titre indépendant, les comptables (surnommés "gatekeepers" en anglais parce qu'ils ont pour rôle de préserver l'intégrité des opérations financières), les négociants en métaux précieux ou pierres précieuses et les fournisseurs de services aux fiducies et aux entreprises. Compte tenu du rôle important de ces entreprises et professions dans les opérations financières, on tend à s'accorder sur le fait que les réglementations visant à réprimer

le blanchiment devraient les viser également dans certaines circonstances, sans préjudice des privilèges liés au secret professionnel.

25. Les centres financiers offshore sont depuis longtemps au cœur des préoccupations relatives à la lutte contre le blanchiment du fait qu'ils peuvent servir de refuges aux blanchisseurs. Or, grâce aux efforts concertés déployés sur le plan international, beaucoup d'entre eux ont déjà corrigé leurs pratiques en retirant leurs licences aux banques écrans ou en renforçant l'obligation d'identifier les clients lorsqu'il s'agit de sociétés. Des campagnes d'information menées aux niveaux national, régional et international ont considérablement contribué à sensibiliser le public aux risques que présente le recours à des centres financiers offshore dont l'organisation et le fonctionnement ne sont pas transparents. Ces centres doivent toutefois continuer d'être contrôlés et surveillés, en raison surtout de la facilité croissante avec laquelle il est possible de faire appel à eux depuis n'importe quel endroit du monde via Internet et d'autres techniques de pointe.

26. Un certain nombre de normes internationales pour la lutte contre le blanchiment sont déjà en place. Comme indiqué précédemment, l'ONU est depuis longtemps un champion de cette cause, à l'origine de plusieurs instruments juridiques importants. Ainsi, en 1988, l'Assemblée générale a adopté une Déclaration politique (résolution S-20/2, annexe) et un plan d'action contre le blanchiment d'argent (résolution S-20/4 D). Dans la Convention contre la criminalité organisée et la Convention contre la corruption, les États parties sont appelés à renforcer leurs systèmes de lutte contre le blanchiment d'argent et le fonctionnement de ces derniers. L'ONU fournit par ailleurs une importante assistance technique dans ce domaine par l'intermédiaire du Programme mondial contre le blanchiment de l'argent de l'ONUDC.

27. Une autre source majeure de normes internationales dans ce domaine est le Groupe d'action financière sur le blanchiment de capitaux. Ses quarante Recommandations, initialement publiées en 1990 puis révisées en 2003, décrivent des normes techniques précises. Le Groupe procède par ailleurs chaque année à un exercice sur les typologies. Il compte un nombre de membres limité, mais des organismes régionaux apparentés aident les autres États de par le monde à appliquer les Recommandations.

28. Parmi les autres sources de normes internationales, on peut citer le Comité de Bâle sur le contrôle bancaire, l'Organisation internationale des commissions de valeurs, l'Association internationale des contrôleurs d'assurances et le Groupe de Wolfsberg, composé de 12 grandes banques privées internationales qui travaillent en coopération avec Transparency International.

29. Ces dernières années, le Fonds monétaire international et la Banque mondiale ont également joué un plus grand rôle dans la lutte contre le blanchiment d'argent et le financement du terrorisme, et ils ont, en coopération avec le Groupe d'action financière sur le blanchiment de capitaux, mis au point une méthode complète d'évaluation du respect des normes.

30. Les établissements financiers ont à leur disposition quantité de renseignements utiles obtenus à l'occasion des opérations commerciales courantes qui sont réalisées à tout moment. À cet égard, un mécanisme systématique et effectif de coopération entre, d'une part, les établissements financiers privés et, d'autre part, les autorités

nationales compétentes est primordial pour traiter efficacement les informations susceptibles de donner lieu à des enquêtes et des poursuites pour blanchiment.

31. Lorsqu'un établissement financier soupçonne ou a des motifs raisonnables de soupçonner que des fonds sont le produit d'une activité criminelle, il devrait le signaler rapidement à un organisme spécialement constitué pour recueillir et traiter ces informations, comme un service de renseignement financier, c'est-à-dire un centre national chargé de recevoir (et, selon qu'il y est autorisé, de demander), d'analyser et de diffuser des informations concernant des opérations suspectes et d'autres informations relatives à d'éventuels cas de blanchiment d'argent. La création d'un tel service est l'une des grandes étapes initiales de la mise en place d'un système national efficace de lutte contre le blanchiment. Les services de renseignement financier dépendent généralement de la banque centrale, du ministère des finances ou de la police, mais l'essentiel n'est pas qu'ils aient tel ou tel organisme de tutelle, mais qu'ils soient pleinement opérationnels. Les déclarations de soupçon sont importantes en ce qu'elles relèvent du devoir de vigilance à l'égard de la clientèle pour repérer les éventuels cas de blanchiment. Les autorités nationales compétentes devraient donner aux établissements financiers des indications pratiques quant aux éléments qui rendent une opération suspecte.

A. Incrimination du blanchiment d'argent: cadre juridique

32. Un cadre juridique efficace est indispensable pour lutter contre le blanchiment d'argent. Les éléments constitutifs de l'infraction de blanchiment sont énoncés dans les instruments juridiques internationaux pertinents, en particulier la Convention de 1988, la Convention contre la criminalité organisée et la Convention contre la corruption. Les États parties sont ainsi tenus d'avoir dans leur législation interne des dispositions permettant d'incriminer les actes qui sont définis dans ces instruments. Ils sont en outre instamment priés de tenir compte des dispositions desdits instruments selon lesquelles la connaissance, l'intention ou la motivation nécessaires en tant qu'éléments d'une infraction peuvent être déduites de circonstances factuelles objectives.

33. Il n'en reste pas moins que la manière dont les États définissent et punissent les activités de blanchiment varie grandement. Pour définir les infractions principales de blanchiment, par exemple, certains États les énumèrent dans une liste annexée à un texte législatif, tandis que d'autres procèdent selon la méthode dite du seuil et les définissent comme des actes passibles de sanctions données. Quoi qu'il en soit, les États parties à la Convention contre la criminalité organisée et à la Convention contre la corruption sont tenus de prévoir un large éventail d'infractions principales.

B. Enquêtes relatives aux infractions de blanchiment d'argent

34. Comme indiqué précédemment, les techniques de blanchiment d'argent ne cessent de progresser tandis que les techniques d'enquête ont tendance à évoluer plus lentement. Il est par conséquent capital pour les enquêteurs d'acquérir les connaissances élémentaires et les compétences nécessaires en matière d'enquêtes sur le blanchiment, s'agissant notamment d'enquêtes scientifiques et de

comptabilité, et de suivre de très près l'apparition de nouvelles méthodes de blanchiment. Surtout, les enquêteurs devraient pouvoir disposer d'équipements techniques adaptés et d'un appui à l'utilisation de ces derniers aux fins de leurs activités quotidiennes, et bénéficier de formations pour leur perfectionnement professionnel. De ce point de vue, il convient d'encourager une fois de plus les pays ayant de bonnes connaissances et compétences en matière d'enquêtes sur le blanchiment à apporter une assistance technique à ceux dont les capacités institutionnelles sont faibles afin qu'ils ne servent de pas de refuges aux auteurs de blanchiment d'argent.

C. Coopération internationale

35. Les infractions financières étant de plus en plus commises d'un côté à l'autre des frontières nationales, le blanchiment d'argent revêt le plus souvent un caractère transnational. Il est toujours difficile, pour les autorités chargées des enquêtes, de détecter des mouvements transnationaux complexes d'argent et d'en établir la preuve; c'est pourquoi la coopération internationale est extrêmement importante dans ce domaine, comme elle l'est pour les enquêtes sur toute autre infraction financière à caractère transnational. Le Groupe Egmont des cellules de renseignement financier, organisation internationale créée pour faciliter la coopération entre services de renseignement financier du monde entier, offre un exemple de coopération de ce type.

D. Mesures de répression visant le produit du crime

36. Les infractions économiques, dont le blanchiment d'argent, étant motivées par la recherche du profit, la localisation, le gel, la saisie et la confiscation du produit du crime sont les mesures les plus efficaces qui puissent être prises à leur encontre. Les dernières séries de mesures que la communauté internationale est convenue d'adopter figurent dans la Convention contre la criminalité organisée et dans la plus récente Convention contre la corruption, en particulier dans le chapitre relatif au recouvrement d'avoirs. Il est urgent de redoubler d'efforts, aux niveaux national et international, pour les étoffer davantage et en exploiter tout le potentiel.

IV. Assistance technique

37. Le Programme des Nations Unies pour la prévention du crime et la justice pénale a principalement pour objet d'aider la communauté internationale à répondre aux besoins pressants qui se font sentir dans le domaine de la prévention du crime et de la justice pénale et d'aider rapidement et concrètement les États à traiter les problèmes liés à la criminalité tant nationale que transnationale.

38. L'une des priorités du programme consiste à étudier le besoin qu'ont les pays en développement et les pays à économie en transition de recourir aux compétences et autres ressources nécessaires pour concevoir et mettre sur pied des initiatives de coopération technique qui soient adaptées aux niveaux national et local.

39. Les ateliers qui se tiendront dans le cadre du onzième Congrès permettront de fournir une assistance concrète sous la forme de contributions directes d'experts et

d'un partage d'informations et de données d'expérience. Ils permettront également d'étudier des idées et projets de coopération technique visant à résoudre les besoins prioritaires et à intensifier l'action menée aux plans bilatéral et multilatéral en matière d'assistance technique et de formation.

40. Pour élaborer des programmes efficaces de coopération technique, il faut disposer de mécanismes et de projets qui soient souples et adaptés aux besoins recensés du pays demandeur et ne fassent pas double emploi avec les activités d'autres entités. En outre, pour combattre efficacement la criminalité économique et le blanchiment d'argent, il faut fournir une assistance technique séquentielle couvrant plusieurs secteurs: sensibilisation et élaboration de politiques; création et mise en œuvre de l'infrastructure juridique appropriée; mise au point de mesures intéressant les secteurs réglementaire et financier; et aide à la mise en application des lois.

41. L'assistance fournie pourra revêtir différentes formes: échange de données de recherche et d'informations; analyse de besoins; services consultatifs; voyages d'étude; séminaires de sensibilisation; élaboration de lois et de règlements types; aide à la rédaction de textes législatifs et réglementaires; stages de formation locaux, nationaux ou régionaux; modules de formation assistée par ordinateur; parrainages et détachements; notes d'orientation et recueils de meilleures pratiques; et soutien et formation aux techniques de communication et d'information. Ces activités pourront être proposées dans le cadre de projets de pays ou régionaux et pourront donner lieu à une coopération locale, bilatérale et multilatérale.

42. L'une des principales difficultés, pour élaborer des programmes opportuns et concrets adaptés à chaque pays, consiste à identifier avec précision les besoins en assistance technique et en formation. Ces informations sont généralement compilées à partir d'un grand nombre de sources et de cadres – études et missions bilatérales et multilatérales d'évaluation des besoins; études de conformité et évaluations réciproques par rapport aux normes mondiales applicables; auto-évaluations; et déclarations faites par les pays dans le cadre de réunions régionales et internationales.

43. Des évaluations de besoins bien conçues peuvent former une base solide pour séquencer et coordonner efficacement l'offre d'assistance. Si certains pays se plaignent parfois d'une "fatigue de l'évaluation", tant en général que par rapport à des activités précises d'assistance technique et de formation, d'autres continuent de demander de telles évaluations, qui doivent les aider à définir et à cerner leurs besoins. En l'absence d'un cadre standard, on peut, pour ce qui est de mettre au point et d'exécuter des évaluations de besoins, renforcer la coopération internationale afin d'améliorer la cohérence des activités et de réduire les redondances.

44. Parallèlement à la collecte d'informations sur les besoins, il faut définir les priorités d'assistance. Une coopération technique ne peut être efficace que si les besoins nationaux et locaux passent, pour ce qui est de déterminer les priorités et les modalités appropriées d'action, avant les impératifs de politique générale ou d'action des organisations donatrices bilatérales ou multilatérales.

45. Pour définir les activités de coopération technique adaptées aux besoins de chaque pays sans faire double emploi avec d'autres mécanismes existants, il faut impérativement mettre en place une coordination efficace. La question de savoir

comment organiser et mettre en œuvre cette coordination a suscité un vif débat au niveau international, en particulier dans le cadre de l'action menée pour combattre le blanchiment d'argent et le financement du terrorisme. Si l'on met souvent en avant la nécessité d'une coordination, on insiste aussi sur le fait que ses mécanismes ne doivent pas entraver l'action menée par les donateurs et prestataires, ni faire "tampon" entre l'État demandeur d'assistance et le prestataire. Pour être efficace, par conséquent, la coordination doit être volontaire et souple, créer de la valeur et non un surcoût, et respecter le mandat de chaque organisation donatrice ou prestataire.

46. Au-delà de la coordination, la nécessité de créer des capacités durables est l'une des principales difficultés auxquelles se heurtent les activités de coopération technique. Cela tient en particulier à la diversité de l'emplacement, de la taille, du développement économique et social, des moyens institutionnels et des systèmes juridiques et administratifs des États Membres. Les pays bénéficiaires demandent constamment que les donateurs et prestataires passent d'activités d'assistance à court terme et à impact limité dans le temps à des activités de formation à plus long terme menées dans les pays, à des détachements, à des voyages d'étude, à la formation de formateurs et à l'envoi de conseillers. L'assistance fournie doit être soutenue sur plusieurs années et, lorsqu'une formation est prodiguée à plus court terme dans un pays ou au niveau régional, elle doit être suivie pour consolider et institutionnaliser les connaissances et les compétences. Dans le domaine de la criminalité économique et du blanchiment d'argent, cependant, on dispose de peu d'experts qualifiés et expérimentés. La communauté internationale doit donc prêter une grande attention à la planification et à la coordination. C'est là, pour les donateurs bilatéraux et multilatéraux, l'occasion de soutenir la mise en place de capacités durables en développant l'offre de formations à plus long terme, de conseillers et de personnels détachés, notamment de techniciens.

47. Pour concevoir des mesures de lutte contre la criminalité économique, y compris le blanchiment d'argent, il importe de tenir compte de la contribution du secteur privé. Les organisations de ce secteur sont souvent l'instrument involontaire de ces délits, mais elles peuvent aussi participer de façon active aux activités de contrôle et de prévention. Dans ces rôles, le secteur privé peut apporter, en matière de coopération technique, une importante contribution aux niveaux national, régional et international. Il reste alors à définir ses possibilités de participation à des activités conjointes d'assistance technique et de formation associant des organisations tant publiques que privées.

V. Conclusions et recommandations

48. L'atelier 5 permettra à la communauté internationale d'étudier des moyens concrets de résoudre plus efficacement les problèmes susmentionnés, compte tenu des propositions faites par les réunions régionales préparatoires au onzième Congrès. Les questions soulevées dans le Guide de discussion établi dans l'optique du Congrès (A/CONF.203/PM.1) serviront également à focaliser la discussion: a) résultats obtenus et obstacles rencontrés dans la répression et la poursuite des affaires de blanchiment d'argent, notamment en ce qui concerne la confiscation du produit d'activités délictueuses opérée conformément aux lois pertinentes; b) comment les services de renseignement financier peuvent collaborer avec leurs

homologues d'autres pays et d'autres institutions pour resserrer la coopération nationale et internationale; et c) mesures à adopter pour appliquer les règles antiblanchiment d'argent dans les secteurs non structurés et les économies où prédominent les opérations en espèces. En outre, l'atelier 5 s'efforcera d'encourager la ratification et l'application de la Convention contre la criminalité organisée et de la Convention des Nations Unies contre la corruption, en particulier pour ce qui est de leurs dispositions relatives au blanchiment d'argent.

49. Dans cette optique, il a été conçu un cas hypothétique devant faciliter le débat interactif entre les participants (voir annexe).

Notes

¹ Adam B. Schiff, dans le compte rendu des travaux menés le 23 mars 2004 par la Sous-Commission de la criminalité, du terrorisme et de la sécurité du territoire national de la Commission des lois de la Chambre des représentants des États-Unis, 108^e Congrès, deuxième session, numéro d'ordre 74, p. 15.

² Synovate, *Identity Theft Survey Report*, rapport établi à l'intention de la Commission fédérale du commerce (septembre 2003), consultable à l'adresse <http://www.ftc.gov/os/2003/09/synovatereport.pdf> (voir p. 4 et 6).

³ Association des banquiers canadiens, "Identity Theft: an old problem needing a new approach" (document inédit), mai 2003, p. 5.

⁴ Nations Unies, *Recueil des Traités*, vol. 1582, n° 27627.

Annexe

Cas hypothétique à examiner lors de l'atelier 5: Mesures de lutte contre la criminalité économique, notamment le blanchiment d'argent

A. Introduction

1. Le cas hypothétique suivant a été imaginé pour faciliter et stimuler la discussion entre les professionnels participant à l'atelier 5, et pour lui donner une orientation concrète en vue de centrer la réflexion sur des mesures de lutte réellement efficaces contre la criminalité économique et le blanchiment d'argent. Ce cas hypothétique soulève différentes questions ayant trait à la prévention, à la collecte d'informations, aux enquêtes et aux poursuites en matière de criminalité économique et de blanchiment d'argent, parmi lesquelles:

- a) Mesures de prévention de la criminalité économique et du blanchiment d'argent;
- b) Informateurs (systèmes d'alerte);
- c) Utilisation des technologies de l'information par les auteurs d'infraction et par les enquêteurs;
- d) Responsabilité des personnes morales;
- e) Usurpation d'identité;
- f) Sociétés écran;
- g) Devoir de vigilance relatif à la clientèle;
- h) Participation aux infractions économiques ou entente en vue de les commettre;
- i) Techniques d'enquête en matière de criminalité économique et de blanchiment d'argent;
- j) Utilisation des technologies de l'information par les auteurs d'infraction et par les enquêteurs;
- k) Coopération interinstitutionnelle;
- l) Coopération internationale, y compris en matière d'entraide judiciaire et d'extradition;
- m) Incrimination du blanchiment d'argent;
- n) Rôle des services de renseignement financier, notamment coopération entre ces services;
- o) Signalement des opérations suspectes;
- p) Types de blanchiment d'argent et modes opératoires;

- q) Questions relatives à l'économie informelle et aux économies où prédominent les opérations en espèces, y compris les systèmes parallèles de transfert de fonds;
- r) Utilisation d'assurances et d'effets de commerce;
- s) Rôle des professionnels dans les activités de lutte contre le blanchiment d'argent;
- t) Mesures de répression visant le produit du crime, notamment gel, confiscation, saisie civile et partage des avoirs;
- u) Restitution aux victimes.

Les personnes désirant participer à l'atelier 5 sont invitées à étudier à l'avance le cas hypothétique décrit ci-dessous.

2. Ce cas est composé de deux parties: la première caractérise un abus de confiance et une escroquerie internationale, infractions qui couvrent plusieurs aspects récurrents de la criminalité économique et peuvent être considérées comme des infractions principales préalables au blanchiment d'argent; la deuxième décrit des activités illégales visant à dissimuler et à déguiser, puis à utiliser le produit du crime provenant des infractions commises dans la première partie.

B. Cas hypothétique

3. Dans l'exemple suivant, les questions soulevées sont indiquées en italiques:

1. Abus de confiance commis par un cadre de banque

- 1. M. Alan est un citoyen du pays Xanadu exerçant des responsabilités dans la banque Finebills Bank, qui est établie dans ce pays.
- 2. M. Banner est également un citoyen de Xanadu et dirige une agence immobilière, Kondo Inc., également établie dans ce pays.
- 3. La situation financière de Kondo Inc. s'étant détériorée, M. Banner demande à M. Alan d'accorder à son entreprise un prêt d'un montant de 1 million de dollars.
- 4. M. Alan étant un vieil ami de M. Banner, il lui accorde le prêt sans lui demander de garanties, tout en sachant qu'il est possible que le prêt ne soit pas remboursé (la décision de M. Alan va alors à l'encontre du règlement intérieur de la banque) (*Renforcement de l'intégrité dans les secteurs public et privé, gouvernement de l'entreprise et autres mesures préventives*).
- 5. Au bout de trois mois, il devient évident que Kondo Inc. ne pourra pas rembourser sa dette (*informateurs ou systèmes d'alertes, dans le cas où cette créance douteuse a été signalée par un employé de la banque*).

2. Fraude à la consommation

- 1. M. Alan craint d'être tenu pour responsable de cette créance douteuse et demande à M. Banner de trouver un moyen de rembourser son prêt.

2. M. Banner consulte sa concubine, M^{me} Chung, qui réside dans le pays Youngland, dont elle est citoyenne, et celle-ci lui propose la solution suivante:
 - a) M^{me} Chung va créer une société écran, Lownet Inc., à Youngland, qu'elle utilisera pour commettre des fraudes à la consommation;
 - b) Elle émettra une publicité par Internet (*utilisation des technologies de l'information*) qui annoncera que Lownet Inc. peut apprendre aux consommateurs comment acheter des biens immobiliers faisant l'objet d'une saisie, et s'engage à fournir le capital nécessaire à ces achats;
 - c) Lownet Inc. s'engagera en outre à verser à chaque client 2 500 dollars pour chaque opération immobilière effectuée en partenariat avec elle et déclarera qu'elle partagera les bénéfices avec ses partenaires après la vente des biens. Elle incitera chaque consommateur à acheter une cassette vidéo de présentation coûtant 60 dollars et promettra une garantie "satisfait ou remboursé" d'une durée de 30 jours. Une partie du million de dollars sera utilisée pour fabriquer les cassettes;
 - d) Lownet Inc. vendra également d'autres cassettes vidéo, beaucoup plus chères que les premières;
 - e) L'objectif de cette publicité sera d'inciter les consommateurs à acheter les cassettes de Lownet Inc., M^{me} Chung n'ayant aucunement l'intention d'aider ses clients à acquérir des biens immobiliers;
 - f) Elle demandera aux clients de payer les cassettes par virement sur le compte bancaire de la société Lownet Inc.;
 - g) Si les clients potentiels lui demandent des renseignements, M^{me} Chung se présentera sous le nom de M^{me} Petal, cadre de la société Lownet Inc., et prétendra que son entreprise a déjà fait affaire à plusieurs reprises avec la banque Finebills Bank, en leur donnant comme référence le nom de M. Alan;
 - h) Lorsque les clients contacteront M. Alan pour se renseigner sur Lownet Inc., celui-ci leur assurera que Lownet Inc. est une société fiable (*responsabilité des personnes morales*)^a;
 - i) M^{me} Chung versera deux millions de dollars à M. Alan et M. Banner si ce projet réussit.
3. M. Alan et M. Banner acceptent la proposition de M^{me} Chung.
4. M^{me} Chung demande à l'un de ses amis, qui est employé dans une banque, comment sont détruits les documents comportant les informations bancaires des clients; celui-ci lui indique que les vieux papiers de la banque sont simplement jetés dans un conteneur situé à

^a La responsabilité juridique de Finebills bank est-elle engagée par les actes de M. Alan?

l'extérieur de la banque (*intégrité organisationnelle*)^b. M^{me} Chung prend dans le conteneur des documents renfermant les informations personnelles de clients de la banque afin d'ouvrir des comptes bancaires dans un autre pays (*usurpation d'identité*)^c.

5. M^{me} Chung crée une société écran, Lownet Inc., (*sociétés écran, rôle des professionnels*)^d dans le pays Youngland, qui est considéré par la communauté internationale comme une place extraterritoriale, et ouvre un compte dans ce pays à la Goldfingers Bank (*participation aux infractions économiques ou entente en vue de les commettre, devoir de vigilance relatif à la clientèle*)^{e,f}.
6. Induits en erreur par la publicité sur Internet, et parfois par la caution apportée par M. Alan, de nombreux clients à travers le monde achètent les cassettes, et le produit de cette entreprise frauduleuse s'élève à cinq millions de dollars, qui sont versés sur le compte de Lownet Inc. à la Goldfingers Bank (*techniques d'enquête, immunité, coopération interinstitutionnelle*)^g.

^b Ce passage soulève la question de la confidentialité des données de l'établissement et de la protection de ces données contre les interventions de tiers.

^c L'usurpation d'identité suppose la collecte de données personnelles en vue de leur utilisation ultérieure à des fins illégales. Le type d'usurpation d'identité illustré dans cet exemple est appelé "dumpster diving" (fouille de poubelles).

^d On pourrait encore débattre de l'usurpation d'identité. Si M^{me} Chung monte la société écran avec l'aide d'un avocat, les participants à l'atelier voudront peut-être discuter, au début de la partie concernant le blanchiment d'argent, du rôle des professionnels dans la prévention de telles activités.

^e En se posant la question de ce qui pourrait être fait si les agents des services de répression avaient connaissance de ce projet avant que les clients n'en soient victimes, les participants à l'atelier pourront réfléchir aux notions d'entente et de participation visées par la Convention des Nations Unies contre la criminalité transnationale organisée.

^f Au début de la discussion sur le blanchiment d'argent, les participants à l'atelier voudront peut-être réfléchir à ce qui aurait dû être fait par la Goldfingers Bank pour empêcher que des comptes ne soient ouverts chez elle par une société écran.

^g Les techniques d'enquête pourraient être étudiées en faisant intervenir dans le scénario un agent des services de répression qui contacterait M^{me} Chung pour obtenir des renseignements en se faisant passer pour un client potentiel. La question de l'immunité pourrait également être abordée à ce stade en se posant la question de savoir ce que pourraient faire les procureurs afin de réunir assez de preuves pour pouvoir engager des poursuites à l'encontre de M^{me} Chung. Les questions relatives à l'entraide judiciaire pourraient également être traitées ici. Enfin, les questions relatives à la coopération interinstitutionnelle pourraient être débattues à ce stade en introduisant dans le scénario des plaintes déposées auprès de l'organisme de protection des consommateurs entraînant l'intervention des services de répression.

3. Blanchiment d'argent et mesures de répression visant le produit du crime

1. M^{me} Chung transfère les 5 millions de dollars déposés à la Goldfingers Bank vers 15 comptes bancaires différents dans le pays Zeitstaat (*signalement des transactions suspectes*)^h.
2. M^{me} Chung remet les informations personnelles qu'elle a recueillies dans le conteneur de la banque à M^{me} Dee et lui demande d'utiliser ces informations pour fabriquer de faux papiers d'identité (*usurpation d'identité*)ⁱ. M^{me} Dee utilise les faux papiers ainsi obtenus pour ouvrir 15 comptes bancaires à Zeitstaat. M^{me} Dee est citoyenne de Zeitstaat, où elle travaille comme comptable (*rôle de filtrage des professionnels*)^j.
3. M^{me} Dee retire les 5 millions de dollars des 15 comptes privés au moyen de nombreux petits retraits effectués dans différents distributeurs automatiques de Zeitstaat et répartis dans le temps (*signalement des opérations suspectes, notamment utilisation des technologies de l'information aux fins de déterminer ces opérations*).
4. À la demande de M^{me} Chung, M^{me} Dee apporte 2 millions de dollars en espèces à Xanadu et les remet à M. Banner. M^{me} Dee ne déclare pas qu'elle transporte 2 millions de dollars aux autorités de Xanadu, pas plus qu'aux autorités de Zeitstaat (*passeurs de fonds, et éventuellement livraison surveillée*), et remet l'argent à M. Banner. Celui-ci verse 1,2 million de dollars sur un compte détenu par Kondo Inc. à la Finebills Bank par petites sommes déposées dans un grand nombre de guichets automatiques (*signalement des opérations suspectes, échange d'informations entre les services de renseignement financier, rôle des institutions financières*). Cette somme est utilisée pour rembourser le prêt de 1 million de dollars ainsi que les intérêts^k. M. Banner garde 400 000 dollars pour son usage personnel et remet la même somme à M. Alan, qui la conserve également pour son usage personnel.
5. M^{me} Dee achète à Zeitstaat, pour le compte de M^{me} Chung et à sa demande, une villa de 2 millions de dollars. Elle lui fait parvenir le reste de l'argent (1 million de dollars) à Youngland par l'intermédiaire d'un banquier occulte, M. Ezura, de Zeitstaat, qui correspond avec M^{me} Jabbar à Youngland (*systèmes parallèles de transfert de fonds*)^l. M^{me} Chung

^h On pourrait relever ici que les critères permettant de reconnaître les opérations suspectes en vue de leur signalement varient d'un État à l'autre, certains ayant établi un montant seuil à partir duquel les opérations doivent être signalées, alors que d'autres ont adopté une approche plus générale, selon laquelle les banques doivent signaler les opérations qu'elles considèrent comme suspectes, quel qu'en soit le montant. Si le virement est effectué par des moyens électroniques, par exemple par SWIFT, il pourrait également être débattu des questions relatives à l'utilisation des technologies de l'information par les blanchisseurs d'argent.

ⁱ Ce point illustre une autre forme d'usurpation d'identité, dans laquelle les données personnelles de tiers sont utilisées pour fabriquer des faux documents et utiliser ces derniers pour commettre de nouvelles infractions (en l'espèce, blanchiment d'argent).

^j Il pourrait être débattu à ce stade de l'incrimination du blanchiment d'argent, notamment, dans le cas de M^{me} Chung, de la question du blanchiment du produit d'infractions commises par le blanchisseur lui-même.

^k On pourrait relever ici que, dans certains États, M. Alan ne serait pas responsable pénalement d'abus de confiance puisque le prêt est remboursé.

remet 10 000 dollars à M^{me} Dee en contrepartie de ses services et dépense 90 000 dollars pour ses loisirs (jeux d'argents, sorties etc.). Elle acquiert des titres au porteur d'un montant de 500 000 dollars auprès de la société Midmint Securities et conserve 400 000 dollars en espèces à son domicile. Ses titres au porteur sont conservés dans un coffre de dépôt à la Handyfunds Bank à Youngland.

6. *Les questions à examiner ont trait, d'une part, au recouvrement par Xanadu, Zeitstaat et Youngland du produit de cette fraude (mesures intérieures et coopération internationale en matière de répression visant le produit du crime, notamment gel, confiscation, saisie civile et partage des avoirs) en vue de leur restitution aux victimes et, d'autre part, à la responsabilité pénale des différents intervenants.*