Nations Unies E/CN.15/2007/8/Add.2

Conseil économique et social

Distr.: Générale
2 février 2007

Français
Original: Anglais

Commission pour la prévention du crime et la justice pénale
Seizième session
Vienne, 23-27 avril 2007
Point 4 de l'ordre du jour provisoire*
Tendances de la criminalité dans le monde et mesures prises: intégration et coordination de l'action que l'Office des Nations Unies contre la drogue et le crime et les États Membres mènent dans le domaine de la prévention du crime et la justice pénale

Résultats de la deuxième réunion du Groupe intergouvernemental d'experts chargé de réaliser une étude sur la fraude et l'abus et la falsification d'identité à des fins criminelles

Rapport du Secrétaire général

Additif

Fraude économique

Table des matières

* E/CN.15/2007/1.

V.07-80546 (F) 280307 290307

IV. Relation entre la fraude économique et d'autres problèmes

A. La fraude et l'implication de groupes de criminels organisés

21. La fraude peut être le fait d'individus, mais les avis des experts et les informations communiquées par les États portent à penser que les cas de fraude les plus graves font intervenir des "groupe de criminels organisés", au sens où cette expression est employée dans la Convention des Nations Unies contre la criminalité transnationale organisée (résolution 55/25 de l'Assemblée générale, annexe I, articles 2 et 3). Les États ont décrit à la fois comment des groupes de criminels organisés établis de longue date se livrent à la fraude et comment de nouveaux groupes sont créés et organisés spécifiquement dans le but de commettre des fraudes et des infractions connexes. Les groupes déjà établis sont attirés par le gain considérable que peut rapporter la fraude, des risques relativement réduits et la possibilité de combiner une fraude à certaines autres des activités criminelles auxquelles ils se livrent. Des groupes plus restreints et plus souples sont constitués pour commettre certains types de fraude comme la fraude sur cartes de débit et de crédit, se déplaçant parfois d'un endroit à l'autre pour éviter d'être découverts par la police ou pour s'attaquer à de nouvelles victimes. Une troisième catégorie est celle des fraudes commises par des personnes morales ou en leur nom. Ainsi, une société ou un groupe d'employés peut être considéré comme un groupe de criminels organisés s'ils commettent une fraude ou s'y trouvent impliqués. Quelques États ont signalé que certains types de fraude attiraient plus que d'autres les groupes de criminels organisés et beaucoup d'États ont considéré la fraude commise par de tels groupes comme plus dangereuse, non seulement parce qu'elle créait un préjudice matériel pour les victimes mais aussi parce que les produits de cette fraude étaient utilisés à des fins de corruption ou pour renforcer de quelque autre manière les activités ou l'influence des groupes de criminels organisés. Cette situation était particulièrement préoccupante dans les pays et les régions en transition, où les institutions étaient plus faibles et où les groupes de criminels organisés bien financés constituaient par conséquent une menace beaucoup plus grave.[1] Un certain nombre d'États considéraient comme plus graves les infractions dans lesquelles se trouvait impliquée la criminalité organisée et avaient prévu des sanctions plus sévères en pareils cas. Plusieurs États ont mentionné que les lois qu'ils avaient promulguées pour combattre la criminalité organisée étaient une mesure qui était et qui pouvait être utile dans les cas de fraude grave; tel était en particulier le cas des lois relatives à des questions comme les pouvoirs d'enquête, le prononcé des peines et l'identification et la confiscation du produit d'activités illicites. L'implication de groupes de criminels organisés signifiait que, le plus souvent, la Convention sur la criminalité organisée pouvait être appliquée pour faciliter l'entraide judiciaire, l'extradition et d'autres formes de coopération lorsque la fraude alléguée avait un caractère transnational. Un certain nombre d'États ont exprimé l'avis que leurs législations existantes étaient suffisantes pour faire face à ce problème, et plusieurs d'entre eux ont souligné la nécessité de poursuivre les travaux dans des domaines comme l'assistance technique et la formation pour que la Convention puisse être utilisée aussi efficacement que possible.

---

[1] Voir la note du secrétariat intitulée "Travaux futurs possibles concernant la fraude commerciale" (A/CN.9/540, par. 3, 8 et 9).

B. Fraude et élément transnational

22. Les États ne disposaient pas d'informations statistiques concernant la fraude transnationale en tant que telle, encore que la fraude de ce type soit commune et que beaucoup d'experts nationaux en aient une longue expérience. Beaucoup d'États ont fait savoir qu'ils avaient rencontré de telles situations et d'autres se sont dits préoccupés par la simple possibilité de s'y trouver confrontés. Les principales craintes étaient que la fraude transnationale était apparemment de plus en plus fréquente et que de telles infractions étaient faciles à commettre mais qu'il était difficile, complexe et coûteux d'enquêter à leur sujet. Quelques États avaient constaté que les délinquants exploitaient délibérément cette difficulté en ne s'attaquant qu'à des victimes se trouvant confortablement hors de portée de leurs propres services de répression.[2] D'autres États ont signalé des exemples de fraudes commises par de petits groupes de délinquants qui se déplaçaient sans cesse, dans le pays même ou à l'étranger, pour s'attaquer à de nouvelles victimes et éviter d'être poursuivis.

23. Un certain nombre d'États ont relevé la relation entre les cas de fraude transnationale et la disponibilité et l'utilisation des technologies de l'information et des communications et des technologies commerciales. Ils ont imputé à la fois la multiplication des cas de fraude en général et l'augmentation de la proportion des cas de fraude comportant un élément transnational à la disponibilité croissante des technologies qui s'offraient aussi bien aux délinquants qu'aux victimes potentielles. La corrélation la plus évidente entre la technologie et l'élément transnational était le fait que des appareils comme le télécopieur ou le téléphone ou des systèmes comme le courriel et l'Internet pouvaient être utilisés par les délinquants pour prendre contact avec leurs victimes, mais il y avait aussi d'autres liens. Un État a relevé que la technologie permettait à des délinquants de pays différents de coopérer efficacement.[3] D'autres ont noté que l'information devant être utilisée pour une fraude devenait un produit illicite et que des listes de victimes potentielles et des données concernant leurs cartes de crédit obtenues par "skimming" ou par d'autres moyens étaient achetées et vendues par des délinquants et souvent transférées par courriel. Un autre lien entre la technologie et l'élément transnational était la pratique consistant pour les délinquants à utiliser des systèmes d'acheminent des appels, des réexpéditeurs anonymes et des moyens semblables pour dissimuler leur identité et l'endroit où ils se trouvaient et éviter d'être dépistés par la police.

24. Plusieurs États ont également décrit des formes de fraude ayant un caractère essentiellement transnational, par exemple la contrebande visant à éluder le paiement de droits de douane, différents types de fraude en matière de transports maritimes, l'immigration clandestine, la falsification de passeports et de visas et la fraude commise par les voyagistes ou les sociétés immobilières, comme la vente de maisons ou d'appartements en temps partagé. L'utilisation de pays tiers était

---

[2] Voir: *Report of the Canada-United States Working Group on Telemarketing Fraud,* (http://www.justice.gc.ca/en/dept/pub/wgtf/headings.html); voir également *Mass-Marketing Fraud: a Report to the Attorney General of the United States and the Solicitor General of Canada,* p. 11-12 (http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf).

[3] Voir *Libman v. the Queen* [1985] 2 S.C.R. 178 (Cour suprême du Canada), et *Secretary of State for Trade v. Markus* [1976] A.C. 35 (Chambre des Lords du Royaume-Uni).

fréquente pour le blanchiment d'argent et certaines formes de fraude fiscale, la comptabilité, d'autres éléments probants ou des avoirs pouvant être ainsi dissimulés hors de portée des enquêteurs. Divers types de fraude sur Internet comportaient également un élément transnational, de multiples pays étant utilisés pour compliquer le dépistage du courriel et d'autres communications.

C. Le rôle des technologies de l'information et des communications et des technologies commerciales

25. La plupart des États n'avaient pas de statistiques concernant le lien qui existait entre l'abus des technologies et la fraude et ne réprimaient pas spécifiquement ce type d'agissements, mais nombre d'entre eux avaient jugé nécessaire de faire en sorte que les définitions existantes de la fraude englobent les innovations technologiques utilisées par les délinquants. Ainsi, les États parties à la Convention du Conseil de l'Europe relative à la cybercriminalité[4] sont tenus de criminaliser la fraude et la falsification informatiques. Il existe des liens évidents entre les technologies de l'information et des communications et les technologies commerciales comme les cartes de paiement et le commerce électronique, ainsi qu'entre les technologies commerciales et de nombreux types de fraude, et la technologie peut être utilisée de bien des façons différentes pour commettre ou faciliter une fraude. L'existence de ces liens a été relevée par la Commission des Nations Unies pour le droit commercial international dans ses travaux sur la fraude commerciale.[5] Les États qui ont communiqué des données ont généralement décrit des types de comportement utilisant beaucoup plus largement les technologies de l'information et ont signalé que les délinquants s'orientaient davantage, peu à peu, vers les technologies commerciales correspondantes et avaient recours aux formes de fraude utilisant ou visant les technologies commerciales et tirant parti des technologies de l'information pour réduire les risques et simultanément accroître les gains illicites et le nombre des victimes. D'autres États, ne disposant pas de données concrètes sur cette question, soit ont signalé que les experts nationaux étaient parvenus à un constat semblable, soit ont fait savoir qu'ils s'attendaient à un tel phénomène ou le craignaient. Les informations statistiques limitées qui sont disponibles sur cette question doivent être abordées avec prudence. L'adoption de nouvelles technologies et pratiques commerciales, les méthodes nouvelles utilisées par les délinquants et l'intervention de la police comme du législateur étaient en effet des éléments qui pouvaient modifier rapidement et de manière imprévisible les taux de délinquance signalés, et les États ont effectivement décrit certains de ces changements. Les différences statistiques sont également dues au fait que les statistiques criminelles sont un domaine en pleine évolution ainsi qu'au fait que la technologie est parfois utilisée pour encourager les victimes à porter plainte, ce qui peut se traduire par une augmentation apparente du nombre d'infractions sans que celui-ci change en réalité.

26. La technologie affecte la fraude de différentes façons. Si elle offre des possibilités nouvelles aux délinquants et réduit les risques auxquels ceux-ci

---

[4] Conseil de l'Europe, *Série des Traités européens*, No. 185, articles 7 et 8.

[5] Voir le rapport de la Commission des Nations Unies pour le droit commercial international sur les travaux de sa trente-sixième session (*Documents officiels de l'Assemblée générale, cinquante-huitième session, Supplément No. 17* (A/58/17), par. 236).

s'exposent, elle peut aussi être très efficace comme moyen de prévention, de maîtrise et de dissuasion de la fraude. Plusieurs États ont relevé que l'impact de la technologie n'était aucunement un avantage exclusif des délinquants. La technologie est la plus communément utilisée par les délinquants pour prendre contact avec les victimes, et notamment pour les identifier et les sélectionner, pour préparer une offre trompeuse, pour obtenir la réponse de la victime et pour assurer le transfert des fonds d'abord de la victime au délinquant puis de celui-ci à d'autres, par exemple pour le blanchir. Dans beaucoup de cas de fraude, des technologies différentes étaient utilisées à diverses étapes de l'opération. Après un premier contact par des moyens de communication ordinaires, il se peut que le délinquant doive, pour convaincre la victime, avoir des contacts plus personnels par téléphone, par exemple. De même, pour que les victimes leur transfèrent des fonds, les délinquants utilisent des moyens de paiement rapides et irrévocables auxquels les victimes ont accès, comme des cartes de crédit ou des virements télégraphiques, mais, par la suite, ils utilisent habituellement d'autres moyens plus difficiles à détecter par les mesures de prévention du blanchiment d'argent. Les délinquants ont également recours à la technologie pour communiquer entre eux, pour transférer des informations comme celles qui concernent des cartes de crédit, pour dissimuler leur identité et l'endroit où ils se trouvent et pour rendre le dépistage des communications aussi difficile que possible. Ils ont aussi recours à des technologies nouvelles comme les numériseurs et les imprimantes pour produire de faux documents de haute qualité, utilisent les moyens technologiques de recherche pour conférer plus de crédibilité à leurs stratagèmes et à différents moyens techniques pour diffuser de fausses informations dans le contexte de larges stratagèmes frauduleux, par exemple pour une fraude dans les enchères ou une fraude sur valeurs mobilières.

27. Aussi bien les États que des entités commerciales privées ont donné des exemples spécifiques et ont fourni des suggestions concernant les technologies pouvant être utilisées pour prévenir la fraude ou pour faciliter les enquêtes et les poursuites, et quelques États ont relevé que ces suggestions faisaient entrevoir un domaine dans lequel les entités publiques et privées pouvaient coopérer efficacement. En général, les méthodes d'enquête technologiquement avancées sont utiles pour le personnel de la police ou du système de justice pénale mais elles mettent parfois les sociétés commerciales devant un dilemme: appuyer la justice pénale tout en protégeant les clients et en veillant à ce que leurs opérations demeurent compétitives et commercialement viables. La mise au point de moyens de lutte contre la cybercriminalité est en soi une vaste activité commerciale et il existe des sociétés qui vendent des conseils et une formation en matière de sécurité et qui mettent au point des technologies destinées à d'autres sociétés qui ont besoin de protéger leurs clients et qui souhaitent éviter des pertes pécuniaires ou autres. Quelques États ont relevé qu'une collaboration étroite était indispensable à toutes les étapes, notamment pour mettre au point de nouvelles technologies commerciales et de nouvelles méthodes de lutte contre la criminalité, la nécessité de disposer d'une large gamme de compétences spécialisées et celle de mobiliser des ressources et d'investir des efforts dans ce que la plupart des États considéraient comme des problèmes en mutation rapide et constante. Les applications technologiques qui ont été mentionnées ont été par exemple les murs pare-feu, la transcription cryptographique et des méthodes d'enquête comme celles qui permettent d'intercepter les communications et d'utiliser les données sur le trafic électronique

pour remonter à la source des communications des délinquants.[6] Un État a noté que les autorités traçaient les communications non seulement pour identifier l'endroit où se trouvaient les délinquants, le produit de leurs activités ou les éléments de preuve, mais aussi pour identifier, dans le cas de fraudes de grande envergure, d'autres victimes n'ayant pas officiellement porté plainte. Une des questions soulevées a été le désir des services de répression de préserver de telles données aussi longtemps que possible, tandis que les entités commerciales, pour leur part, se préoccupaient généralement des coûts que représentait la conservation de telles informations ainsi que de ses incidences sur la confidentialité des clients et des abonnés. Un certain nombre d'États ont également évoqué la possibilité d'utiliser différentes technologies afin de prévenir la fraude en faisant rapidement connaître les stratagèmes connus et les faits nouveaux afin d'alerter les services de police, les sociétés privées et les victimes potentielles. Il ressortait des recherches menées par différentes sociétés privées que la plupart des cas de fraude commerciale, y compris les cas de fraude faisant intervenir l'utilisation de technologies de pointe, reposaient sur la participation d'employés initiés, ce qui mettait en relief la nécessité de dispenser une formation pour que les intéressés sachent reconnaître les cas de fraude et les prévenir, ainsi que l'importance qu'il y avait à protéger les intérêts des entreprises privées et des clients.

D. Fraude, produits de la fraude et blanchiment d'argent

28. La fraude et le blanchiment d'argent sont liés mais la plupart des États les considèrent comme des problèmes distincts. La fraude était considérée comme un délit économique car son objet était de produire un avantage financier autre pour les délinquants, tandis que le blanchiment d'argent, bien qu'il s'agisse d'une opération réalisée dans un environnement économique, n'était pas considéré comme une forme de délit économique car son but était de dissimuler et de transférer le produit d'activités illicites seulement après que ce profit ait déjà été réalisé au moyen d'autres délits. Indépendamment des informations qu'ils ont fournies au sujet des lois pertinentes, la plupart des États ayant répondu au questionnaire ne se sont pas étendus sur les mesures de lutte contre le blanchiment d'argent. D'un point de vue de procédure, quelques États ont relevé que si la fraude et le blanchiment d'argent étaient liés et s'il fallait les combattre de manière coordonnée, le blanchiment d'argent faisait déjà l'objet d'études détaillées de la part d'autres organes et que les travaux futurs concernant la fraude devraient éviter tous chevauchements d'efforts inutiles. La plupart des États ont considéré que la fraude était l'une des infractions sous-jacentes qui déclenchaient l'application des mesures de lutte contre le blanchiment d'argent: 30 États avaient qualifié une ou plusieurs infractions frauduleuses graves d'infractions principales, 12 États n'ont pas fourni d'informations à ce sujet, et 4 seulement ne considéraient pas la fraude comme une infraction principale aux fins des mesures de lutte contre le blanchiment d'argent. Les États ont évoqué dans leurs réponses une large gamme de dispositions civiles et

---

[6] Voir par exemple l'alinéa d) de l'article 1 de la Convention du Conseil de l'Europe sur la cybercriminalité: "'données relatives au trafic' désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent".

pénales et de procédures concernant la présentation de preuves qui avaient été promulguées en matière de gel, de saisie, de confiscation et de restitution du produit d'activités frauduleuses. Les principaux points à prendre en considération dans le contexte de la fraude étaient notamment la nécessité d'évaluer le coût global de la fraude aux échelons national et mondial et les sommes qu'elle générait, l'importance relative de la fraude en comparaison des autres infractions comme source des fonds blanchis et la destination ultime du produit de la fraude. En outre, des préoccupations ont été exprimées par des sociétés commerciales et certaines associations de défense des victimes à propos de la différence entre la confiscation du produit d'activités criminelles et le recouvrement par les entreprises des pertes subies.

29. Quelques États seulement ont fourni des informations concernant le montant total des pertes subies ou du produit généré par la fraude, mais les montants en jeu étaient manifestement substantiels, certains États citant des chiffres comme plusieurs centaines de millions de dollars pour le produit de la fraude et des milliards de dollars pour le total des pertes subies.[7] Les sources commerciales citées provenaient seulement d'un petit nombre de secteurs comme celui des assurances et celui des cartes de crédit, mais leurs conclusions correspondaient à ces chiffres. Le Groupe d'action financière sur le blanchiment de capitaux (GAFI) ne publie pas de statistiques ni d'estimations détaillées mais considère généralement la fraude et les formes connexes de délinquance financière parmi les quatre types de crime générant le plus gros bénéfice illicite, les trois autres étant le trafic de stupéfiants, le trafic d'armes et le trafic de migrants et la traite de personnes.[8] Obtenir des informations exactes sur le montant global du bénéfice généré par la fraude et les autres infractions soulevaient apparemment un défi formidable. Les services nationaux de renseignement financier opéraient en faisant enquête sur les transactions financières apparaissant comme suspectes ou relevant d'autres catégories, comme les opérations en espèces de grande envergure, mais les informations obtenues étaient utilisées pour les enquêtes et non à des fins statistiques. Au stade de l'enquête, il était habituellement difficile de dire si des fonds étaient blanchis et, lorsque tel était le cas, quelle était l'infraction à laquelle se rapportaient les fonds en question. En outre, les statistiques nationales sur la criminalité étaient généralement fondées sur le nombre d'affaires, de poursuites, de condamnations et de peines. Le produit des opérations frauduleuses, lorsqu'il était connu, pouvait habituellement faire l'objet d'une estimation seulement, et ces estimations ne reflétaient habituellement que les transactions et les victimes connues, qui ne représentaient qu'une petite proportion du total réel dans la plupart des cas. Les informations les plus précises qui soient disponibles concernant le produit de la fraude se trouvent entre les mains d'entreprises privées, qui suivent les pertes subies pour leur propre gestion. Mais ces informations ne concernent que les activités spécifiques de ces entreprises et elles sont parfois considérées comme confidentielles. En outre, les pertes effectivement causées par la fraude sont bien supérieures aux bénéfices empochés par les délinquants. Le montant du bénéfice réalisé n'est pas toujours intégralement signalé,

---

[7] Voir "Travaux futurs possibles sur la fraude commerciale: note du secrétariat" (A/CN.9/540), par. 5-11.

[8] Voir Groupe d'action financière sur le blanchiment de capitaux, *Rapport sur les typologies de blanchiment d'argent, 1995-1996* (Paris, Organisation de coopération et de développement économiques, juin 1996), par. 10 et 11; et Ibid., *Rapport sur les typologies de blanchiment d'argent, 2000-2001* (Paris, OCDE, février 2001), par. 52 et 53.

détecté ou compté et le calcul des pertes subies peut englober les coûts indirects, qu'une entreprise commerciale a qualifiés de "dommages accessoires".[9]

30. La fraude et le blanchiment d'argent sont conceptuellement différents mais peuvent se ressembler dans la pratique.[10] La principale différence est que la fraude consiste essentiellement à convertir des fonds légaux en gains illicites, tandis que le blanchiment d'argent est une opération qui a pour but de transférer et de dissimuler le bénéfice déjà réalisé, bien que ni la fraude ni le blanchiment d'argent soit habituellement aussi simple dans la pratique. Par exemple, de l'argent apparemment blanchi provenant d'une victime peut être payé à d'autres comme "produit de leur investissement" pour les attirer ou pourrait même être payé à la même victime pour l'encourager à participer à l'opération ou pour éviter qu'elle ne porte plainte devant les autorités. La principale similitude tient au fait que l'un et l'autre font fréquemment intervenir des tromperies et des transactions clandestines ou dissimulées. La tromperie inhérente à ces deux délits et leur ressemblance créent parfois des difficultés pour les services de répression mais peuvent également leur offrir un moyen d'action. Plusieurs États ont fait observer que les mécanismes mis en place pour combattre le blanchiment d'argent, comme l'obligation de déclarer les transactions suspectes, peuvent également être employés ou adaptés pour découvrir les cas de fraude, et certaines banques, institutions commerciales ou financières et entreprises de télécommunications vérifiaient déjà les données concernant les transactions afin de déceler tout schéma inhabituel qui porterait à soupçonner des cas de fraude. Comme dans le cas d'autres infractions sous-jacentes, la fraude peut parfois déclencher des enquêtes et des poursuites pour blanchiment d'argent et inversement, ce qui met en relief la nécessité d'une coopération entre les entités publiques et privées appropriées.

31. La plupart des États ont fait savoir qu'ils avaient promulgué des dispositions législatives prévoyant la confiscation du produit de la fraude et d'autres délits. Ces dispositions avaient notamment mis en place différents systèmes fondés sur la condamnation pénale des délinquants, des procédures *in rem*, des procédures hybrides selon lesquelles une confiscation civile pourrait être fondée sur une condamnation pénale ou des actions civiles en recouvrement entamées par les victimes ou, dans un cas au moins, par l'État. Un État s'est référé à un système selon lequel la réparation des pertes subies, lorsqu'elle ne pouvait pas être obtenue des délinquants, pouvait être réclamée à l'État lui-même. Le recouvrement et la restitution du produit d'activités criminelles peuvent susciter dans la pratique des problèmes majeurs, spécialement dans le cas de fraudes commerciales de grande envergure et de fraudes massives. Dans le cas de fraudes commerciales, les victimes sont fréquemment des personnes morales et, indirectement, des investisseurs, des actionnaires et des clients dont les droits peuvent être difficiles à définir. Dans le cas de fraudes massives, le grand nombre de petites réclamations concurrentes présentées devant des instances multiples peut entraîner une procédure si complexe que les dépenses afférentes à l'évaluation du préjudice, à l'action judiciaire proprement dite et à la restitution du produit de la fraude peuvent dépasser le montant du préjudice subi ou l'argent disponible pour verser une indemnisation. L'action civile peut également se heurter à des obstacles majeurs, qui tiennent

---

[9] Price Waterhouse Coopers Global Economic Crime Survey 2005, sect. 3.3.

[10] Voir Groupe d'action financière sur le blanchiment de capitaux, *Rapport sur les typologies de blanchiment d'argent, 2000-2001*, par. 13 et 58.

notamment au fait que les pouvoirs inhérents à la justice pénale et les recours visant à obtenir le gel, la saisie et la confiscation du produit de la fraude ne sont généralement pas disponibles.

E. Relation entre fraude et corruption

32. Les États n'étaient pas invités, dans le questionnaire, à communiquer des informations sur le lien entre la fraude et la corruption, mais, dans leurs réponses, ils ont néanmoins évoqué certaines relations entre les deux. Ces relations étaient notamment les situations dans lesquelles un comportement criminel relevant à la fois des dispositions réprimant la fraude et réprimant la corruption et les situations où, alors même que les infractions étaient couvertes par des textes différents, il existait des liens factuels entre les deux types d'infractions. Par exemple, une fraude commise par une personne de l'extérieur pouvait être considérée comme une escroquerie mais comme un détournement de fonds lorsqu'elle était imputable à un employé. La plupart des États ayant fourni des informations concernant les exemples de fraudes transnationales de grande envergure ont relevé que ce type de fraude était habituellement le fait de groupes de criminels organisés, ce qui permettait de penser que le produit de la fraude était utilisé pour financer d'autres activités de ces groupes, par exemple pour verser des pots-de-vin ou corrompre des agents de police afin d'éluder l'action des pouvoirs publics. Les États ont également évoqué le paiement de pots-de-vin dans le contexte de la fraude en matière de passation de marchés, et notamment la corruption des agents chargés de prévenir et de signaler les transactions frauduleuses. Un État a relevé que sa législation considérait plusieurs formes communes de corruption comme fraude contre l'État ou le gouvernement. Les types de fraude devant être criminalisés en vertu de la Convention des Nations Unies contre la corruption (résolution 58/4 de l'Assemblée générale, annexe)[11] peuvent constituer des formes de fraude dans certaines circonstances ou y être liés, en ce sens que la corruption peut être commise dans le cas d'une fraude, ou bien le produit d'une fraude peut être utilisé pour corrompre des agents publics. Indépendamment du détournement de biens par un agent public, par exemple, l'infraction qu'est le recel de biens acquis à la suite d'un acte de corruption (article 24) peut être difficile à distinguer du recel à des fins de fraude. Le trafic d'influence (article 18) peut également être considéré comme une forme de fraude, en ce sens qu'un agent public qui vend son influence vend en fait, dans la pratique, quelque chose qui ne lui appartient pas et qu'il n'a pas le droit de vendre, et est considéré comme une forme de fraude contre l'État par au moins un des États ayant répondu au questionnaire.

---

[11] Résolution 58/4 de l'Assemblée générale, annexe. Les infractions devant être criminalisées en vertu de la Convention contre la corruption sont notamment la corruption d'agents publics (articles 15, 16 et 21), le détournement de biens par un agent public (articles 17 et 22), le trafic d'influence (article 18), l'abus de fonctions (article 19), le blanchiment d'argent (article 23), le recel (article 24) et l'entrave au bon fonctionnement de la justice (article 25).

F. Relation entre fraude et terrorisme

33. À la différence de la falsification d'identité, qui peut avoir des motifs non économiques, par exemple un désir de dissimulation, la fraude économique est commise en vue d'un gain matériel, ce qui la rend utile pour les terroristes, essentiellement comme moyen de financer leurs organisations ou leurs opérations.[12] Dans ses rapports, l'Équipe d'appui à l'analyse et de surveillance des sanctions créée en application de la résolution 1526 (2004) du Conseil de sécurité, qui est responsable de la surveillance des sanctions imposées à Al-Qaeda et aux Taliban, considère la fraude ainsi que d'autres infractions comme les enlèvements, les extorsions de fonds, les vols à main armée et le trafic de stupéfiants comme des sources potentielles de fonds pour les terroristes.[13] La même série de crimes a été signalée par le Groupe d'action financière dans ses travaux relatifs au financement du terrorisme.[14] Plusieurs États ont fait savoir qu'ils avaient rencontré des cas de fraude, bien que rares, qui étaient liés et dont il y avait des raisons de penser qu'ils étaient liés à des activités terroristes, et d'autres États ont dit être préoccupés par ce problème. De petites opérations locales de fraude et la fraude sur cartes de crédit étaient utilisées, ou soupçonnées de l'être, pour financer les opérations d'individus ou de petits groupes, tandis que des stratagèmes plus sophistiqués de fraude sur cartes de crédit pouvaient servir à financer des opérations plus vastes ou à générer des ressources plus substantielles et plus soutenues pour d'autres activités.[15] Les sources d'information consultées pensent que la tendance est peut-être à des opérations frauduleuses ou d'autres infractions de portée plus réduite et plus locale comme source de fonds étant donné que, plus fréquemment, les activités terroristes ne coûtent pas cher, que les activités transnationales de grande envergure peuvent plus facilement être détectées et qu'Al-Qaeda est devenue une organisation fragmentée.[16]

34. Les cas de fraude économique de grande envergure cités par les États ont été notamment des cas de fraude concernant la fraude à l'assurance, la contrebande et la fraude aux impôts indirects, la fraude dans des opérations de change, la fraude à la sécurité sociale et la fraude commerciale. La fraude à la sécurité sociale et la fraude sur carte de crédit sont utilisées à la fois comme moyens de se procurer directement

---

[12] S'il n'existe pas de consensus concernant la définition du "terrorisme" en général, ce terme est précisé, aux fins des infractions liées au financement du terrorisme, à l'article 2 de la Convention internationale pour la répression du financement du terrorisme (Nations Unies, *Recueil des Traités*, vol. 2178, No. 38349). La question de savoir quelles étaient la définition et la portée de l'expression "terrorisme" a été laissée aux États Membres, et il est difficile de dire si les informations communiquées par les États étaient fondées sur la Convention ou sur les définitions et descriptions utilisées par les États eux-mêmes.

[13] Voir la résolution 1267 (1999) du Conseil de sécurité, le troisième rapport de l'Équipe d'appui à l'analyse et de surveillance des sanctions créée en application de la résolution 1526 (2004) concernant Al-Qaeda, les Taliban et les personnes et entités qui leur sont associées (S/2005/572), par. 69 et 70; et le quatrième rapport de l'Équipe (S/2006/154), par. 63 à 66.

[14] Voir Groupe d'action financière sur le blanchiment de capitaux, *Rapport sur les typologies de blanchiment d'argent, 2001-2002* (Paris, Organisation de coopération et de développement économiques, février 2002), par. 10 à 12.

[15] Ibid., par. 11, exemple 1.

[16] Voir le troisième rapport de l'Équipe d'appui à l'analyse et de surveillance des sanctions (S/2005/572), par. 67 à 70; et Mark Rice-Oxley, "Why terror financing is so tough to track down", *Christian Science Monitor*, 8 mars 2006.

des ressources pour de petites opérations terroristes locales et comme sources de financement pour de vastes opérations bien organisées. Plusieurs États se sont également dits préoccupés par la fraude dirigée contre les prestataires de services de télécommunications, le motif réel étant en l'occurrence non pas d'obtenir des services gratuits mais plutôt d'avoir accès à des services Internet ou des services de courriel ou encore des services de téléphonie mobile anonymes dont la source ne peut être identifiée. Ce type de fraude est habituellement le fait des cybercriminels et des criminels organisés, mais les organisations terroristes ont maintenant commencé à utiliser les mêmes méthodes pour les mêmes raisons.[17]

35. Dans leurs réponses, plusieurs États se sont dits particulièrement préoccupés par le risque que des organisations philanthropiques soient frauduleusement utilisées pour financer le terrorisme, et quelques-uns ont cité des cas dans lesquels ce type de fraude avait été détecté ou soupçonné. L'abus d'organisations philanthropiques et autres organisations à but non lucratif par des organisations terroristes a également été jugé préoccupant par le Groupe d'action financière,[18] ainsi que par les experts et journalistes.[19] Indépendamment de la fraude et du détournement des contributions versées à ces organismes caritatifs pour mobiliser des fonds, ces organismes ont été utilisés comme moyens de blanchir de l'argent ou de transférer secrètement des fonds provenant d'autres sources.[20] Le Comité contre le terrorisme du Conseil de sécurité a relevé les difficultés particulières auxquelles se heurtaient les États ayant entrepris, conformément à la résolution 1373 (2001) du Conseil de sécurité, de réprimer l'abus d'organisations à but non lucratif comme moyen de se procurer ou d'acheminer des fonds destinés à des activités terroristes.[21] En 2004, la liste globale des personnes et entités soumises aux mesures visant à tarir les sources de financement d'Al-Qaeda et des Taliban comprenait 17 organisations caritatives ou organisations à but non lucratif qui menaient 75 opérations dans 37 États.[22]

36. Les deux scénarios les plus préoccupants sont la création d'organismes caritatifs fictifs qui financent directement le terrorisme, qui est une tromperie à l'égard des donateurs, ainsi que l'infiltration d'organisations caritatives légitimes afin de détourner les dons vers le terrorisme, soit par le biais d'une fraude, soit au

---

[17] Voir par exemple le témoignage de Richard A. Rohde devant la Sous-Commission de la technologie, du terrorisme et de l'information publique de la Commission des affaires judiciaires du Sénat des États-Unis d'Amérique, 24 février 1998 (http://www.fas.org/irp/congress/1998_hr/s980224r.htm); et Alan Sipress, "An Indonesian's prison memoir takes holy war into cyberspace: in sign of new threat, militant offers tips on credit card fraud", *Washington Post*, 14 décembre 2004.

[18] Voir Groupe d'action financière sur le blanchiment de capitaux, *Recommandations spéciales concernant le financement du terrorisme* (22 octobre 2004), recommandation spéciale VIII; et Groupe d'action financière sur le blanchiment de capitaux, *Annexes 2002-2003*, annexe B, section intitulée "Lutte contre l'abus des organisations à but non lucratif".

[19] Voir par exemple Martin Rudner, "Using financial intelligence against the funding of terrorism", *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), p. 42 et 43; et Jeremy Scott-Joynt, "Warning signs for the funding of terrorism", *BBC News* (http://news.bbc.co.uk/2/hi/business/4692941.stm).

[20] Martin Rudner, "Using financial intelligence against the funding of terrorism", *International Journal of Intelligence and Counter Intelligence*, vol. 19, No. 1 (2006), p. 43-44.

[21] Voir le rapport du Président du Comité contre le terrorisme sur les problèmes rencontrés dans l'application de la résolution 1373 (2001) du Conseil de sécurité (S/2004/70, annexe), sect. II. A.

[22] Voir le troisième rapport de l'Équipe d'appui à l'analyse et de surveillance des sanctions (S-2005/572), par. 84.

moyen d'un vol pur et simple. Les organisations caritatives légitimes connaissent également des difficultés. Il est en particulier difficile pour elles de se conformer à des normes comptables rigoureuses, ce qui accroît leurs frais généraux, et même des rumeurs dépourvues de fondement selon lesquelles elles seraient impliquées dans des cas de fraude ou de terrorisme peuvent beaucoup contribuer à faire hésiter les donateurs. Le fait que les États et les organisations caritatives ne disposent pas des moyens nécessaires pour combattre l'infiltration de celles-ci et le détournement des contributions par des groupes terroristes apparaît comme un problème sérieux à la fois pour les organisations elles-mêmes pour les États sur le territoire desquels est essentiellement réalisée l'œuvre menée au moyen des contributions versées à ces organisations.[23]

37. Un autre aspect est celui des organisations caritatives qui s'occupent de communautés religieuses, ethniques ou culturelles spécifiques et des causes liées à des régions en conflit car les fonds de ces organisations risquent d'être détournés vers les groupes terroristes, outre que les normes comptables et les normes de supervision sont particulièrement difficiles à appliquer. Il peut être difficile, en pareils cas, d'établir une distinction entre la fraude et d'autres infractions. L'utilisation des dons à des fins terroristes est généralement considérée comme une fraude si les donateurs sont trompés et comme une extorsion de fonds si les donateurs ne sont pas trompés mais plutôt intimidés. Lorsque les donateurs savent quel est l'objet véritable de l'organisation et n'agissent pas sous la contrainte, aussi bien les donateurs que l'organisation caritative bénéficiaire peuvent commettre des infractions réprimées par la législation nationale relative au financement du terrorisme et par les mesures adoptées pour mettre en œuvre la Convention internationale pour la répression du financement du terrorisme.[24] Outre le rôle qu'elles peuvent jouer comme source de fonds, les organisations caritatives peuvent être utilisées comme circuits d'acheminement de fonds générés par d'autres infractions ou provenant de sources licites, auquel cas il y a violation des mesures réprimant le financement du terrorisme ou le blanchiment d'argent.

G. Relation entre la fraude économique et la délinquance liée à la falsification d'identité

38. Pour éviter les chevauchements, la relation entre la fraude économique et la délinquance liée à l'usurpation d'identité est discutée dans l'additif au présent document concernant ce dernier type de délit (E/CN.15/2007/8/Add.3, par. 13 et 14).

H. Impact de la fraude dans les pays en reconstruction ou en transition

39. La fraude économique et les formes connexes de corruption ont suscité des problèmes supplémentaires dans les pays où les structures économiques fondamentales ont été affaiblies ou dans les pays qui traversent une période de transition, et les États en ont donné plusieurs exemples. Lorsqu'un pays traverse une

---

[23] Ibid., par. 85 à 88.

[24] Nations Unies, *Recueil des Traités*, vol. 2178, No. 38349.

situation de transition économique majeure, de développement, de reconstruction ou de redressement après un conflit ou une catastrophe naturelle, la situation peut être plus favorable à la fraude qu'aux efforts visant à la prévenir, à la dissuader ou à la maîtriser. En pareilles situations, les mesures de sauvegarde visant à prévenir la fraude et la corruption peuvent se trouver affaiblies, de nouvelles possibilités pour l'une et l'autre peuvent apparaître et le préjudice causé par les cas de corruption ou de fraude, surtout lorsqu'elle est de grande envergure, peut être plus sérieux que si la même infraction était commise dans un contexte différend. Les pertes économiques provoquées par des fraudes de grande envergure peuvent être suffisamment importantes pour ébranler une économie déjà affaiblie ou déstabilisée par d'autres problèmes, tandis que les gains financiers provenant de telles opérations peuvent considérablement renforcer des groupes de criminels organisés qui se trouvent déjà en présence de systèmes de justice pénale affaiblis, situation qui ne fait qu'encourager la corruption et susciter d'autres problèmes. Le succès de ces fraudes de grande envergure et la présence d'une corruption généralisée peuvent éroder la confiance dans les nouvelles structures économiques et entraver la mise en œuvre des réformes. La fraude est également un délit qui repose sur la tromperie, et les possibilités de tromperie se multiplient dans les pays en transition, où les nouvelles règles et pratiques sociales et économiques ne sont pas toujours bien comprises. Dans certains cas, des conflits et des catastrophes naturelles majeures créent également des possibilités pour les délinquants étant donné que de vastes sommes d'argent sont mobilisées auprès d'organisations caritatives et d'autres sources et doivent être dépensées rapidement là où les mesures de lutte contre la fraude et la corruption qui seraient autrement applicables sont difficiles à mettre en œuvre ou peu efficaces.

40. Il peut y avoir un lien étroit entre la fraude et la corruption et, dans certains cas, les deux infractions sont identiques ou se chevauchent. Par exemple, l'appropriation de fonds destinés à un projet de développement est habituellement considérée comme une fraude mais, si ce délit est commis par une personne de l'intérieur, il peut s'agir d'un détournement de fonds.[25] Dans d'autres cas, ces infractions peuvent être séparées mais être reliées par les agissements des délinquants. Comme dans le cas de la passation des marchés et des autres formes de fraude plus communes, les fraudeurs soudoient fréquemment une personne de l'intérieur pour s'assurer que la fraude réussisse sans être découverte.

41. Les États et les experts ont signalé plusieurs exemples de telles situations. Il a notamment été signalé des cas de fraude dans le contexte de projets de reconstruction et de projets de réforme dans les pays en transition, notamment dans le contexte des nouveaux régimes fiscaux, des nouveaux processus de passation des marchés et des programmes de privatisation. Un État a déclaré avoir découvert des cas de fraude dirigée contre le fisc et les programmes de privatisation dont le produit avait constitué une source majeure de fonds pour des groupes de criminels organisés. Un autre État a signalé un cas de fraude au nouveau processus de remboursement de la taxe sur la valeur ajoutée qui avait été suffisamment sérieux pour affecter le budget national. Les fraudeurs ont également exploité les efforts de reconstruction financés au moyen des contributions caritatives internationales et des primes d'assurance après des catastrophes naturelles majeures tel le tsunami qui a

[25] Voir par exemple la *Convention contre la corruption*, articles 17 et 21.

déferlé en Asie en 2004[26] et, dans deux cas au moins, d'importants cas de fraude "à la boule de neige" avaient contribué à déstabiliser des pays en transition.[27]

V. Coopération internationale et compétence

42. Les cas de fraude transnationale de grande envergure constituent un sérieux défi pour la coopération internationale. Ces cas de fraude doivent habituellement donner lieu à des enquêtes vastes, complexes et coûteuses relevant de plusieurs pays et faisant intervenir de nombreux délinquants, un grand nombre de victimes et de services d'enquête ainsi que d'institutions du secteur privé. Dans les États où les règles et pratiques suivies en matière de coopération ont évolué pour pouvoir faire face à un petit nombre d'affaires de grande envergure, des fraudes massives peuvent être dissimulées de manière à apparaître comme un grand nombre de fraudes relativement modestes. Lorsqu'elle aboutit, la fraude génère un bénéfice substantiel qui peut être utilisé pour soutenir des groupes de criminels organisés, protéger les opérations frauduleuses en cours, dissimuler et blanchir le produit obtenu et organiser de longues procédures de recours pour faire obstacle à l'entraide judiciaire et à l'extradition. Nombre des observations reçues ont mis en relief la nécessité d'une coopération, mais l'avis général a été que les instruments juridiques existants et surtout la Convention sur la criminalité organisée et, pour les États qui y sont parties, la Convention du Conseil de l'Europe sur la cybercriminalité, constituaient un fondement juridique suffisant pour cette coopération et que l'accent devrait être mis sur des options et des mesures visant à faire en sorte que les instruments disponibles puissent être et soient utilisés plus efficacement plutôt que de vouloir en élaborer de nouveaux. Il a été relevé en outre, dans certains importants domaines de coopération contre la fraude, et surtout en matière de prévention, qu'aucune autorisation formelle du législateur ni aucun fondement juridique quel qu'il soit n'était nécessaire.

---

[26] Plusieurs services nationaux de police se sont spécifiquement attaqués aux fraudeurs cherchant à exploiter les efforts de secours; par exemple, l'ancien Service national de renseignement criminel du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord a publié un avis public ("Menace de fraude après le tsunami: Avis au public"). Voir également la page web du Federal Bureau of Investigation des États-Unis ("Tsunami disaster relief fraud alert: don't be scammed", http://www.fbi.gov/page2/jan05/tsunamiscam010505.htm). Le Ministère de la justice des États-Unis a créé après le cyclone Katrina une équipe spéciale chargée de s'attaquer à différents types de fraudes, comme celles visant les organisations caritatives, les fonds de prestation des secteurs public et privé, les compagnies d'assurance, les procédures de passation des marchés et de prévenir la corruption et les cas d'usurpation d'identité en vue d'obtenir des prestations (http://www.usdoj.gov/katrina/Katrina_Fraud/index.html).

[27] Après l'effondrement d'un plan d'investissement "à la boule de neige", pendant la période 1996-1997, l'Albanie a connu des problèmes graves, dont une flambée de violence et le pillage d'armes légères détenues par les arsenaux de l'État (voir Carlos Elbirt, "Albania under the Shadow of the pyramids", *Transition Newsletter*, 2001, http://www.worldbank.org/html/prddr/trans/so97/albania2.htm). De même, certaines sources citent l'effondrement d'un même type de plan, sanctionné par l'État, comme ayant contribué à la chute du Gouvernement haïtien en 2004.

A. Entraide judiciaire et autre forme de coopération en matière d'enquêtes

43. Plusieurs États ont mis en relief le fait que, d'une manière générale, il importait de garantir l'efficacité de l'entraide judiciaire. Les enquêteurs et les services du parquet ont habituellement besoin d'informations et d'éléments de preuve concernant les communications échangées entre les délinquants et les victimes et les virements de fonds, en particulier des informations permettant d'identifier la source et la destination des communications entre les délinquants et les victimes et le contenu de ces communications afin de pouvoir prouver des éléments constitutifs de l'infraction comme une tromperie. Les états financiers documentant les virements de fonds sont nécessaires aussi. Il importe de remonter jusqu'à l'origine du produit de la fraude, y compris les virements initiaux des victimes aux délinquants, ainsi que les opérations réalisées par la suite pour blanchir les fonds obtenus. Il importe par ailleurs de rassembler des éléments établissant le préjudice causé par les cas de fraude transnationale de grande envergure, et il pourra s'agir par exemple d'éléments de preuve directe apportés par des victimes ou bien d'éléments rassemblés par des experts spécialisés. Des experts pourront devoir être appelés à témoigner pour établir que le comportement des délinquants sortait des usages commerciaux normaux. Plusieurs États ont soulevé la question des moyens à employer pour transférer des preuves testimoniales, et les experts ont appelé l'attention sur l'utilisation de conférences vidéo, conformément aux dispositions de la Convention sur la criminalité organisée.[28] Pour être efficace, la coopération visant à lutter contre la fraude n'exige pas toujours une entraide judiciaire formelle car certaines communications et certains échanges d'éléments de preuve peuvent être interceptés dans le pays où l'enquête a été ouverte. Les principaux problèmes recensés dans ce domaine tenaient notamment à la complexité des affaires et à la durée de la coopération requise. Plusieurs États ont souligné qu'il fallait permettre aux enquêteurs de coopérer rapidement et de manière informelle. La plupart des formes de coopération supposaient des échanges d'information et il fallait par conséquent concilier les besoins de l'enquête et les garanties appropriées. Un État a noté que s'il était fréquemment important de pouvoir échanger rapidement des informations dans les cas de fraude transnationale, il importait aussi d'adopter une approche équilibrée et transparente pour que les informations échangées soient exactes et soient utilisées conformément aux règles juridiques pertinentes.

B. Extradition

44. La plupart des États ont fait savoir qu'ils pouvaient extrader les personnes soupçonnées d'avoir commis des actes criminels et certains d'entre eux ont fait savoir qu'ils étaient habilités à poursuivre les infractions commises en dehors de leur juridiction territoriale lorsqu'ils ne pouvaient pas extrader les intéressés. Certaines des raisons données pour justifier les refus d'extradition, comme l'interdiction d'extrader des nationaux, des lois d'amnistie et les délais de

---

[28] Voir *Report of the Canada-United States Working Group on Telemarketing Fraud* et le paragraphe 18 de l'article 18 de la Convention sur la criminalité organisée, qui prévoit l'utilisation de conférences vidéo pour la prise de dépositions. Des dispositions semblables se trouvent au paragraphe 18 de l'article 46 de la Convention contre la corruption.

prescription, pouvaient devenir des obstacles dans les affaires de fraude. Les experts ont relevé que le paragraphe 5 de l'article 11 de la Convention sur la criminalité organisée prévoyait de longs délais de prescription pour les affaires dans lesquelles étaient impliqués les groupes de criminels organisés, spécialement lorsque ceux-ci s'étaient soustraits à la justice, et essentiellement les mêmes raisons ont été invoquées dans le contexte des affaires de fraude les plus complexes.

45. Aux termes de la Convention sur la criminalité organisée, les États parties sont tenus d'extrader les délinquants accusés des formes les plus graves de fraude ou de les poursuivre, sous réserve des exclusions visées à l'article 16 de la Convention, mais l'obligation de poursuivre ne s'applique que si la raison du refus d'extradition tient à la nationalité du délinquant. Les conditions essentielles qui doivent être remplies pour que l'extradition puisse être accordée sont que le type de fraude commise soit considéré comme un crime grave par la législation interne des deux États parties et que le crime commis implique un groupe de criminels organisés et ait un caractère transnational.[29] Aux termes de la Convention, les États parties sont également tenus de veiller à avoir compétence sur les infractions commises au-delà de leur juridiction territoriale par l'un de leurs ressortissants lorsqu'ils ne peuvent pas l'extrader pour des raisons de nationalité et de permettre le transfèrement de délinquants condamnés pour qu'ils purgent leurs peines dans leurs pays d'origine.[30] Les États parties sont également encouragés à établir leur compétence à l'égard des infractions commises par un accusé qui se trouve sur leur territoire mais qu'ils n'ont pas l'intention d'extrader, mais cela n'est pas obligatoire.[31] Les lacunes qui existent dans le contexte de la Convention pourraient être comblées, notamment en encourageant tous les États parties à mettre en œuvre intégralement la Convention et à veiller à ce que les cas de faute grave soient considérés comme des crimes graves, et en encourageant les États parties qui n'extradent pas leurs nationaux à appliquer le principe *aut dedere aut judicare*. Il existe une autre lacune potentielle dans le cas de deux autres scénarios. Les États doivent se montrer disposés à poursuivre les fraudeurs qui ne sont pas extradés exclusivement pour le motif que ce sont des nationaux, conformément au paragraphe 4 de l'article 15 facultatif et ils doivent avoir les moyens de le faire. Enfin, la plupart des cas de faute grave impliquent des groupes de criminels organisés, mais des infractions transnationales peuvent également être commises par des individus et elles pourraient être poursuivies dans le contexte d'accords ou d'arrangements ponctuels. La Convention du Conseil de l'Europe sur la cybercriminalité[32] prévoit également l'extradition dans les cas où les États intéressés sont parties, et cela n'est pas limité aux États qui sont membres du Conseil. Cependant, aux termes de la Convention, l'extradition du chef d'infractions comme la fraude et le faux et l'usage de faux n'est possible que dans certaines circonstances, lorsque l'infraction dont il s'agit fait intervenir l'usage d'ordinateurs

---

[29] Alinéas a) et b) de l'article 2 et paragraphe 2 de l'article 3 de la Convention sur la criminalité organisée.

[30] Paragraphes 3 et 4 de l'article 15, paragraphes 1 et 10 de l'article 16 et article 17 de la Convention sur la criminalité organisée; voir les *Guides législatifs pour l'application de la Convention des Nations Unies contre la criminalité transnationale organisée et les Protocoles y relatifs* (publication des Nations Unies, numéro de vente: F.05.V.2) ainsi que la discussion des questions de compétence figurant dans le "rapport explicatif" de la Convention sur la cybercriminalité, par. 233 et 239 (http://conventions.coe.int/Treaty/en/Reports/html/185.htm).

[31] Paragraphe 4 de l'article 15 de la Convention sur la criminalité organisée.

[32] Articles 3 et 4 (criminalisation) et 24 (extradition) de la Convention sur la cybercriminalité.

ou de systèmes ou de données informatiques. Cependant, la Convention sur la cybercriminalité n'est pas limitée aux affaires dans lesquelles se trouve impliqué un groupe de criminels organisés et peut être appliquée lorsqu'une falsification ou une fraude informatique est commise par un individu.

C. Compétence

1. Compétence territoriale

46. La fraude transnationale est l'une des formes de délinquance qui présentent le plus fréquemment des difficultés du point de vue de la compétence territoriale classique.[33] Il se peut que les infractions soient planifiées dans un pays et commises par des délinquants basés dans un deuxième pays et soient dirigées contre des victimes se trouvant dans un troisième pays encore et que le produit de la fraude soit accumulé et blanchi dans un quatrième pays. Les victimes résident souvent dans des pays très divers et d'autres pays peuvent être utilisés pour d'autres fins, par exemple pour transférer des fonds ou comme base des sites Internet frauduleux. Dans les affaires transnationales les plus sophistiquées, les délinquants savent quelles sont les limites de la compétence nationale et sont tout à fait capables de structurer leurs opérations de manière à tirer le maximum de parti des lacunes ou des faiblesses éventuelles. Face à cette situation, les concepts de compétence territoriale ont évolué eux aussi et cette compétence s'est trouvée élargie de manière à englober des infractions commises dans deux ou plusieurs pays simultanément, se poursuivant d'un pays à l'autre ou commises d'un pays mais ayant un impact tangible dans un autre. L'affirmation de compétence à l'égard d'une infraction dont l'exécution a commencé dans l'État qui a entamé les poursuites et qui a été parachevée ailleurs, ou bien une infraction dont un élément essentiel est exécuté dans ledit État est aujourd'hui chose commune.[34] Quelques États fondent leur compétence territoriale sur le lieu où l'infraction a été préparée ou sur le lieu où le dernier élément ou tout élément essentiel de l'infraction a été exécuté, notamment lorsque le lieu où l'infraction a effectivement été commise est incertain.[35] Il est plus difficile de dire si la compétence peut être fondée sur la présence d'éléments non essentiels de l'infraction sur le territoire d'un État. Un seul État a signalé la possibilité d'aller plus loin.[36] Dans cet État, l'existence d'un lien authentique et substantiel avec le territoire doit être établi, y compris la présence d'éléments non essentiels comme la planification, la préparation ou la présence du produit de l'infraction, mais il n'est

---

[33] Voir par exemple Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003) p. 158-180.

[34] John Seguin, "The case for transferring territorial jurisdiction in the European Union", *Criminal Law Forum*, vol. 12, No. 2 (2001), p. 249.

[35] Voir par exemple la *Loi de 1993 relative à la justice pénale* du Royaume-Uni (c. 36), partie I (http://www.opsi.gov.uk/ACTS/acts1993/Ukpga_19930036_en_1.htm); et Michael Hirst, *Jurisdiction and the Ambit of the Criminal Law*, Oxford Monographs on Criminal Law and Justice (Oxford, Oxford University Press, 2003), p. 163 et suivantes.

[36] Au Canada, la condition liée à l'existence d'un "lien authentique et substantiel" avec le territoire est fondée sur la jurisprudence. L'affaire concernait une fraude préparée au Canada mais dirigée contre des victimes se trouvant dans d'autres pays. La compétence était fondée sur le fait que la fraude avait été préparée au Canada et que son produit avait été rapatrié par l'entremise d'autres pays, mais certains éléments essentiels de l'infraction avaient également été commis dans le pays (voir *Libman c. la Reine* [1985] 2 S.C.R. 178 (Cour suprême du Canada)).

pas certain que la compétence puisse être fondée exclusivement sur de tels facteurs. Les législations nationales qui exigent la présence d'un élément essentiel comme fondement de la compétence territoriale dépendent aussi pour une large part des modalités selon lesquelles les infractions ont été préparées et de la question de savoir quels sont les éléments considérés comme essentiels. Les infractions de type entente sont habituellement plus larges, par exemple, la préparation d'infractions relevant de la cybercriminalité et d'infractions faisant intervenir les systèmes de télécommunications peuvent expressément comprendre des éléments comme le type d'effet et d'impact qui doivent avoir lieu à l'intérieur du territoire d'un État pour que celui-ci puisse exercer sa compétence. L'article 11 de la Convention du Conseil de l'Europe sur la cybercriminalité érige en infraction pénale la tentative et la complicité en vue de la perpétration d'une des infractions établies conformément à la Convention, y compris la falsification et la fraude informatiques.

47. Il arrive fréquemment que les motifs de poursuites les plus solides se trouvent dans les pays où résident les victimes et sur le territoire desquels se produisent les effets de l'infraction. Beaucoup d'États affirment leur compétence sur le fait que le résultat ou l'impact de l'infraction s'est produit sur leur territoire. La plupart d'entre eux limitent ces effets à ceux qui sont jugés essentiels aux éléments factuels de l'infraction, ce qui, dans le cas de la fraude, signifie habituellement la présence des victimes. Certains appliquent parfois une version plus large du même principe en englobant les pertes indirectes. C'est ainsi par exemple qu'une fraude contre une société peut affecter ses actionnaires ou les marchés. Les principaux obstacles aux poursuites, spécialement dans le cas de fraudes de grande envergure sont les coûts et la complexité des enquêtes, le principe *ne bis in idem* et le fait que des éléments essentiels comme des témoins et des preuves doivent être importés et peuvent ne pas répondre aux normes nationales en matière de preuve. Même lorsqu'un État est juridiquement compétent, de tels obstacles peuvent l'empêcher d'exercer sa compétence et l'amener à entamer des pourparlers avec d'autres États pour déterminer quelle est l'instance devant laquelle des poursuites peuvent le plus facilement être entamées.

48. La nature de la fraude elle-même et le fait que les délinquants essaient de tirer parti des lacunes et des limites qui restreignent la compétence des États lorsqu'ils préparent et mènent à bien leurs stratagèmes suscitent des difficultés sérieuses dans le contexte des concepts existants de compétence territoriale. D'une part, la nécessité de veiller à ce que les infractions puissent effectivement faire l'objet de poursuites et celle d'éviter des lacunes de compétences que puissent exploiter les délinquants conseillent un modèle de compétences relativement large. D'un autre côté, les risques de conflits de compétence et les problèmes liés aux coûts et à la complexité des poursuites d'infractions transnationales portent à penser qu'une approche plus prudente serait mieux appropriée. La tendance à l'expansion progressive de la compétence territoriale se poursuivra sans doute du fait, en partie de l'imagination que reflètent les affaires de fraude traditionnelle et de l'accès toujours plus facile aux technologies de l'information. Il est peu probable que l'on trouve une seule formule simple permettant de déterminer la compétence dans tous les cas possibles et il n'existe actuellement aucun modèle applicable à toutes les affaires pouvant être envisagées. La meilleure solution consiste probablement à veiller à ce qu'un nombre d'États aussi grand que possible appliquent un concept de compétence territoriale relativement large, à ce que les divers États concernés

collaborent efficacement et à ce que ce soit l'État qui est le mieux placé pour le faire qui entame effectivement les poursuites.

49. Pour faire en sorte que les cas de fraude transnationale puissent faire l'objet de poursuites efficaces, il existe un certain nombre de possibilités sur le plan juridique et pratique, selon les mesures qui ont déjà été promulguées dans chaque État. Ces mesures tendent notamment à garantir l'existence d'une compétence suffisante sur la base des différents modèles de juridiction envisagés dans le présent rapport et, lorsqu'il y a lieu, d'éléments non essentiels comme le lieu où l'infraction a été planifiée et préparée et où se trouve le produit de la fraude, éléments qui peuvent être plus importants en l'occurrence que dans le cas d'autres types de délits. La formulation de lois réprimant la fraude est importante aussi, surtout lorsque la compétence territoriale est fondée sur les éléments essentiels considérés comme constitutifs de l'infraction. Dans le cas de fraude menée à partir d'un pays ou commise en utilisant le territoire d'un pays qui ne dispose pas de moyens nécessaires en matière d'enquêtes ou de poursuites, il pourrait être offert une assistance technique de caractère général afin de renforcer les capacités nécessaires, et une assistance pourrait être offerte aussi pour combattre des infractions spécifiques dans le cadre de la coopération internationale.

50. Étant donné les revendications de compétence existantes, il arrive fréquemment que plusieurs États puissent affirmer leur compétence et il sera pour eux important de se consulter pour déterminer quel est celui d'entre eux qui devra entamer des poursuites. Ces consultations pourront porter sur des questions juridiques, diplomatiques ou pratiques allant de la solidité relative des communications de compétence et autres revendications juridiques de chaque État et de la question de savoir si les délinquants peuvent être extradés vers l'État qui souhaite mener des poursuites à des considérations pragmatiques comme les coûts et les obstacles à prévoir s'agissant de transférer des éléments de preuve d'un État à l'autre, d'assurer leur recevabilité et de faire en sorte qu'ils soient présentés de façon convaincante devant le tribunal. Lorsqu'il est décidé lequel de plusieurs États possibles doit entamer les poursuites, les autres États peuvent lui transférer leur compétence. C'est ce que prévoit le Traité type relatif au transfert de procédures en matière pénale (résolution 45/118 de l'Assemblée générale, annexe), l'article 21 de la Convention sur la criminalité organisée et l'article 47 de la Convention des Nations Unies contre la corruption (résolution 58/4 de l'Assemblée générale, annexe).[37] Lorsque deux ou plusieurs États ont compétence et veulent entamer des poursuites, l'on pourrait envisager d'appliquer les critères ci-après:

a) *État qui a subi le préjudice direct et indirect le plus substantiel*. Le préjudice constitue à la fois un encouragement et une justification des poursuites et signifie habituellement que des éléments de preuve seront disponibles;

b) *État sur le territoire duquel la plupart des éléments de l'infraction* ont été commis;

c) *État qui a investi le plus dans l'enquête sur l'affaire*. Indépendamment du volume des ressources engagées, cela signifie habituellement que l'État a en sa possession les éléments de preuve nécessaires pour mener à bien des poursuites;

---

[37] Voir également John Seguin, "The case for transferring territorial jurisdiction in the European Union" *Criminal Law Forum*, vol. 12, No.2 (2001), Seguin, loc. cit., p. 249.

d) *Lieu où se trouvent les témoins et les éléments de preuve*. Le transfert de volumes considérables d'éléments de preuve, surtout dans le cas de fraudes complexes ou massives, renchérit considérablement l'opération et peut avoir un impact sur la recevabilité des preuves et sur la possibilité d'utiliser celles-ci de manière efficace;

e) *État dont le dossier est le plus solide*. Compte tenu de l'ensemble des preuves qui peuvent être rassemblées dans chaque État ou transférées à chacun d'eux, des lois relatives à la preuve de chaque État et de critères semblables, il peut apparaître qu'un État a plus de chances que d'autres d'obtenir une condamnation;

f) *État ayant le plus de moyens*. Du fait de la complexité des cas de fraude de grande envergure, les coûts de l'opération et les compétences requises peuvent solliciter beaucoup les enquêteurs et les services du parquet. Les États qui ont une longue expérience et suffisamment de ressources peuvent envisager soit d'assumer la compétence à l'égard de l'affaire, si cela est juridiquement possible, ou de fournir une assistance à un autre État dont le dossier est plus solide et dont les moyens sont moindres;

g) *Nationalité du délinquant et possibilité de l'extrader*. Les États dont le dossier est à d'autres égards moins solide pourront devoir poursuivre leurs propres ressortissants s'ils ne peuvent pas être extradés;

h) *Autres infractions en cause ou pouvant être poursuivies*. Si la compétence est habituellement liée à des infractions spécifiques, les fraudes de grande envergure comportent également d'autres infractions, dont des infractions liées à l'usurpation d'identité ou le blanchiment d'argent. Dans certains cas, il peut y avoir intérêt à déterminer l'État qui est le mieux placé pour poursuivre ensemble toutes les infractions relevant de l'affaire;

i) *Autres délinquants en cause ou pouvant être poursuivis*. De même, il peut y avoir intérêt, dans des cas particuliers, de déterminer quel est le for le plus commode pour poursuivre plusieurs membres d'un groupe criminel et d'extrader ensuite les autres pour les juger tous ensemble;

j) *Régimes respectifs en matière de condamnation*. Généralement, un État peut se montrer disposé à céder sa compétence à d'autres États qui appliquent des sanctions similaires aux infractions commises, mais ils cèdent moins volontiers leur compétence à des États qui appliquent des sanctions qu'ils peuvent considérer comme excessivement rigoureuses ou au contraire indulgentes.

2. Compétence extraterritoriale

51. Les concepts de compétence territoriale se sont élargis pour suivre l'évolution de la fraude et des autres délits transnationaux les plus communs, mais l'application d'une compétence extraterritoriale en matière de fraude est moins usuelle. Certains États appliquent une compétence extraterritoriale lorsqu'un délit est commis à l'étranger par un de leurs ressortissants ou par une personne ayant son domicile sur leur territoire ou d'autres liens avec ledit territoire, surtout si leur constitution interdit l'extradition de nationaux.[38] La compétence fondée sur la nationalité des

[38] Les États parties à la Convention sur la criminalité organisée et à la Convention contre la corruption qui ne peuvent pas extrader leurs nationaux sont tenus d'affirmer cette compétence

victimes (personnalité passive) est possible aussi, bien qu'en matière de fraude économique, un tel fondement juridique puisse être difficile à distinguer de celui qui est à la base de la compétence territoriale fondée sur les faits ou les résultats de la fraude. Quelques États ont signalé avoir adopté le concept de compétence extraterritoriale pour protéger ce qu'il considérait être les intérêts vitaux contre des types spécifiques de fraude, sur la base du principe de protection. Parmi les exemples à citer, il y a lieu de mentionner la contrefaçon de monnaie, de passeports ou d'autres documents essentiels et la fraude affectant les systèmes nationaux d'immigration. Un autre domaine qui n'a pas été mentionné et qui pourra conduire à invoquer le principe de protection est celui de fraude de grande envergure contre un gouvernement, qui pourrait également être considéré comme relevant de la corruption.

D. Délais de prescription

52. Les experts ont relevé que les délais de prescription pourraient poser un problème dans nombre d'affaires de fraude en raison du temps nécessaire pour pouvoir faire enquête et poursuivre des affaires transnationales complexes, et ils ont pris note des dispositions de la Convention sur la criminalité organisée et de la Convention contre la corruption[39] aux termes desquelles les parties doivent établir des délais de prescription appropriés compte tenu des infractions visées par la Convention et des cas dans lesquels le délinquant s'est soustrait à la justice. Les experts ont envisagé plusieurs approches pour assurer l'application de délais de prescription appropriés, notamment l'établissement par la loi de délais de base appropriés eu égard aux infractions frauduleuses auxquelles ils s'appliquent, la suspension des délais dans certaines circonstances, par exemple lorsque le délinquant a retardé la procédure ou s'est soustrait à la justice, et la promulgation de dispositions législatives permettant aux juges de prolonger un délai de prescription dans les circonstances spécifiques prescrites par la loi. La formule consistant à autoriser le juge à prolonger les délais a été considérée comme incompatible avec le principe fondamental *nullum crimen sine lege* par certains experts, et d'autres qui ont vu un risque qu'il soit porté atteinte aux droits garantis par des lois fondamentales. Cette formule n'a donc pas été considérée comme une option viable.

E. Coopération en matière de prévention

53. Pour une large part, la coopération internationale contre la fraude concerne des mesures à postériori, comme les enquêtes et les poursuites, lorsque la fraude a déjà commencé ou s'est déjà produite. La plupart des États n'ont pas évoqué la prévention dans les informations qui sont communiquées au sujet de la coopération internationale. Celle-ci peut néanmoins jouer un rôle important dans la prévention à différents égards, et le coût et la complexité des enquêtes et des poursuites dans le cas de fraudes transnationales de grande envergure portent à penser que les

---

(voir le paragraphe10 de l'article 16 et le paragraphe 3 de l'article 15 de la Convention sur la criminalité organisée ainsi que le paragraphe 11 de l'article 44 et le paragraphe 3 de l'article 42 de la Convention contre la corruption).

[39] Voir le paragraphe 5 de l'article 12 de la Convention sur la criminalité organisée et l'article 29 de la Convention contre la corruption.

dividendes produits par des efforts concertés de prévention peuvent être substantiels. La fraude transnationale consiste en activités entreprises sur le territoire de divers États et peut habituellement être évitée au moyen de mesures nationales si les autorités appropriées disposent en temps voulu des informations nécessaires pour la prévenir. La coopération internationale en matière de prévention de la fraude comprend les éléments de caractère général ou au contraire spécifique. Au plan général, la fourniture d'une assistance pour la mise au point et le perfectionnement de méthodes de prévention, l'échange des enseignements retirés et des pratiques optimales et le partage des informations nécessaires pour mettre au point ces techniques et en améliorer l'efficacité sont autant d'éléments importants. En outre, des informations peuvent être échangées au sujet de cas spécifiques, des méthodes utilisées par les délinquants ou des cas de fraude découverts, ce qui n'englobe pas nécessairement les types d'informations de nature personnelle ou d'informations recueillies dans le cadre des enquêtes qui exigent un processus formel d'entraide judiciaire.

VI. Coopération entre les secteurs public et privé

54. La fraude économique est un délit du commerce. Le secteur commercial et la justice pénale doivent par conséquent collaborer et ont tout intérêt à le faire. Dans son rapport sur les travaux de sa trente-sixième session, la Commission des Nations Unies pour le droit commercial international (CNUDCI) a relevé la nécessité d'une telle collaboration et a demandé à la Commission sur la prévention du crime et la justice pénale d'agir tandis que la CNUDCI poursuivrait ses propres travaux; c'est cet appel qui a débouché, entre autres, sur la présente étude.[40] Cependant, les pratiques et les objectifs de la justice pénale et du commerce ne coïncident pas toujours. Certaines formes de fraude commerciale peuvent ne pas être érigées en infractions par le droit pénal. Lorsque les intérêts de la justice pénale tendent à privilégier les enquêtes, les poursuites et le châtiment, les intérêts commerciaux tendent à privilégier les mécanismes de règlement des différends ou le recouvrement des pertes subies. L'élément commun est un intérêt immédiat à agir rapidement pour mettre fin aux opérations frauduleuses en cours et un intérêt stratégique prééminent, à savoir la prévention et la répression à la fois de la fraude et des groupes de criminels organisés, qui paraissent être à l'origine d'une proportion importante des cas de fraude.

55. Dans d'autres domaines, néanmoins, les intérêts publics et privés divergent. Tandis que les intérêts privés sont régis par le commerce, le marché et les obligations fiduciaires à l'égard des actionnaires, les intérêts publics sont de caractère plus général, et des considérations non commerciales comme les droits de l'homme, la protection de l'environnement ou le bien commun ont tendance à prédominer. Le maintien de l'état de droit et d'institutions judiciaires et pénales efficaces exige que des fonctions clés, en particulier les poursuites et les fonctions judiciaires, demeurent à l'abri d'influences extérieures. Si une coopération efficace est importante, il est essentiel de mettre en place des garanties adéquates pour

---

[40] *Documents officiels de l'Assemblée générale, cinquante-huitième session, Supplément No. 17* (A/58/17), par. 238 à 241; voir également le paragraphe 6 de la résolution 2006/24 du Conseil économique et social, et les *Documents officiels du Conseil économique et social, 2004, Supplément No. 10* (E/2004/30), par.82.

veiller à ce que les intérêts commerciaux ne compromettent pas l'indépendance de la magistrature du siège et du parquet. En sens stratégique général, les secteurs public et privé ont un intérêt commun dans l'efficacité des systèmes de justice pénale. En outre, les valeurs et les institutions qui sont à la base de l'état de droit sont essentielles à la gouvernance et à la réglementation du commerce ainsi qu'à la création et au maintien d'environnements sociaux et économiques stables dans lesquels les entreprises commerciales puissent prospérer.

56. Il ressort des réponses des États qu'il est à la fois très nécessaire d'élargir la coopération entre les secteurs public et privé et qu'il existe à cet égard de larges possibilités. La plupart des États n'ont guère fourni d'informations au sujet de la coopération mais beaucoup ont souligné qu'ils la jugeaient nécessaire. Un certain nombre d'États n'ont décrit que les mesures de caractère contraignant, comme l'obligation imposée par la loi de signaler les infractions aux autorités ou de faire connaître à celles-ci les personnes morales ou les employés impliqués dans des opérations frauduleuses. Plusieurs États ont mentionné les normes réglementaires et législatives applicables. Les États-Unis d'Amérique ont décrit la loi qu'ils avaient promulguée en 2002 pour définir les normes visant à prévenir la fraude et à améliorer la gouvernance des sociétés.[41] Plusieurs autres États ont mentionné les dispositions de leurs codes de commerce et des réglementations adoptées pour encourager l'application de normes et de pratiques visant à dissuader et à prévenir la fraude. Ces réglementations, entre autres, avaient pour but de promouvoir la publication d'états financiers transparents et l'audit des entreprises, d'encourager les personnes ayant connaissance d'irrégularités à les signaler et à coopérer avec les autorités ou à imposer aux cadres supérieurs la responsabilité de l'exactitude des informations comptables et financières publiées. Un petit nombre d'États ont signalé avoir élaboré des stratégies nationales de développement du commerce et de l'industrie comportant notamment des dispositions relatives à la fraude ou à d'autres problèmes de délinquance d'intérêt commun. Ces stratégies prévoyaient des consultations ou des réunions à l'occasion desquelles des experts du commerce et de la justice pénale pouvaient s'entretenir pour identifier les problèmes émergents et élaborer des approches communes ou concertées. Quelques États ont également fait savoir que des organes consultatifs mixtes avaient été constitués pour s'attaquer à des problèmes spécifiques comme la fraude et le blanchiment d'argent.

57. L'existence de mesures contraignantes n'est pas nécessairement un reflet du climat général qui caractérise la relation entre les secteurs public et privé. Plusieurs États ont déclaré avoir promulgué des dispositions législatives imposant aux entreprises privées de protéger le caractère confidentiel des informations personnelles qui leur sont communiquées dans le cadre de leurs activités, et beaucoup de sociétés pouvaient voir leur responsabilité civile engagée si elles communiquaient des informations confidentielles (à moins d'être obligées à le faire par la loi). Dans beaucoup de pays, cependant, il existait apparemment de larges possibilités d'élaborer des normes réglementaires et d'adopter en matière commerciale et en matière de justice pénale des pratiques de prévention contre la fraude de caractère concerté plutôt que contraignant fondées sur des consultations entre les entités appropriées des secteurs public et privé. Le domaine de

[41] Loi des États-Unis sur la réforme de la comptabilité des sociétés quotées en Bourse et sur la protection des investisseurs (Loi Sarbanes-Oxley de 2002) (Pub. L. 107-204, 116 Stat. 745, U.S.C., titre 15, articles 7201 et suivants).

collaboration le plus fréquemment mentionné a été l'échange d'informations entre entités commerciales. Celles-ci sont fréquemment les premières à avoir connaissance des nouveaux cas de fraude, soit parce que leurs clients les signalent, soit parce qu'elles constatent des types d'activités et des pratiques commerciales inhabituelles, et il a été jugé important que ces entités alertent sans tarder les autorités pour que celles-ci puissent sans tarder ouvrir une enquête et adopter les mesures requises pour mettre fin aux opérations frauduleuses en cours. L'autre principal domaine de collaboration potentielle était celui de la prévention. Les mesures visant à prévenir la fraude, qui sont évoquées dans la section VII ci-après, peuvent en gros être classées en deux catégories: les mesures concernant des victimes potentielles, l'intention étant de rendre une tromperie plus difficile, et les mesures concernant des structures commerciales spécifiques, pour qu'il soit plus difficile pour les délinquants de les attaquer ou de les exploiter.

VII. Prévention de la fraude économique

58. Dans leurs réponses au questionnaire, les États ont mentionné toute une série de mesures de prévention pouvant être adoptées. Comme la fraude repose sur une tromperie des victimes, quelques États ont mentionné dans leurs réponses les campagnes d'information mises sur pied pour alerter et éduquer les victimes potentielles. Les autres mesures mentionnées en matière de prévention ont été notamment des mesures ayant recours à la technologie pour rendre la fraude plus difficile et pour accroître les possibilités de découvrir rapidement les cas de fraude et y faire échec avant que ces opérations ne causent un grand nombre de victimes. Plusieurs États ont relevé l'importance que revêtaient des moyens d'échange rapide d'informations exactes pour pouvoir mettre en œuvre rapidement avec quelques chances de succès des efforts d'éducation et de prévention. Quelques États ont mentionné l'éducation de personnes autres que les victimes potentielles, en particulier les employés des établissements bancaires et des institutions financières, qui étaient parmi les premiers à avoir connaissance des cas de fraude. Certains États ont relevé que les méthodes visant à contrecarrer le blanchiment d'argent et la corruption pouvaient utilement contribuer à prévenir la fraude et à en atténuer les effets. Un État a noté que le fait d'interdire aux personnes reconnues coupables de fraude de se livrer à nouveau à des activités commerciales (par exemple en refusant de leur octroyer les permis ou patentes nécessaires) pourrait décourager les récidivistes. Un autre État a relevé qu'aussi bien les entreprises que les clients pouvaient prendre des précautions simples, par exemple en faisant en sorte qu'il ne soit pas possible de modifier l'adresse postale et de faire suivre le courrier, ce qui pourrait beaucoup contribuer à prévenir la fraude.

59. Plusieurs États ont été d'avis que les mesures techniques de sécurité pourraient être importantes du point de vue de la prévention. La création et l'utilisation de systèmes modernes de transcription cryptographique, par exemple, étaient ce qui avait rendu possible l'emploi des technologies modernes de paiement par cartes de crédit, et les milieux d'affaires internationaux avaient joué un rôle de pionnier en ce qui concerne l'utilisation de signatures numériques et d'autres adaptations pour réduire la fraude dans le contexte de transactions commerciales importantes.[42] De

[42] Voir la Loi type sur les signatures électroniques élaborée par la Commission des Nations Unies

telles mesures techniques apparaissaient comme nécessaires dans presque tous les domaines du système commercial, qu'il s'agisse des éléments se trouvant entre les mains des usagers, des communications entre les divers maillons du système et les dispositifs de traitement et d'entreposage des données. Il a été relevé en outre qu'en raison de la portée mondiale du commerce et des systèmes d'identification, la plupart des mesures techniques devaient être appliquées à l'échelle mondiale, car des mesures de sécurité qui ne le seraient que dans un pays ne produiraient aucun effet dans d'autres ou risqueraient d'empêcher totalement l'utilisation légitime d'une carte de crédit ou d'autres technologies. Un autre des problèmes que soulevait la mise au point de nouvelles techniques de sécurité était l'évolution constante de la technologie, des applications commerciales et des méthodes employées par les délinquants. Aussi était-il essentiel que les entités tant publiques que privées ne relâchent jamais leur vigilance et consacrent l'effort et les ressources nécessaires à la mise au point et à la diffusion de nouvelles mesures de prévention dès que les mesures existantes devenaient obsolètes.

60. La mise au point et l'application de mesures techniques de prévention pouvaient également soulever des questions de coûts et de compétitivité pour les entreprises commerciales. La question de savoir si les mesures de lutte contre la délinquance, surtout celles qui se rapportent aux enquêtes et aux poursuites, devraient être payées par l'État ou par les entreprises et les usagers des technologies suscite parfois des controverses. Les entreprises commerciales tendent à peser leurs options en termes de rapport coût-avantages et craignent parfois que l'adoption de certaines mesures de sécurité ne nuisent à leur compétitivité sur les marchés mondiaux étant donné que leurs concurrents d'autres pays pouvaient ne pas être soumis aux mêmes exigences. C'était sans doute aux marchés qu'il convenait de laisser le soin de dicter la mise au point et l'utilisation des mesures de prévention technique, mais l'État avait néanmoins un certain rôle à jouer. Beaucoup d'États ont indiqué qu'ils fixaient des normes minimums pour mettre le consommateur à l'abri de la fraude et des pratiques connexes comme la publicité trompeuse ou mensongère et certains d'entre eux fixaient également des normes minimums pour garantir la protection des informations concernant les clients. Les États peuvent jouer un rôle utile, aussi bien individuellement que collectivement, en veillant à ce que le marché encourage l'adoption de mesures de prévention et de sécurité efficaces et que ces mesures ne compromettent pas la compétitivité et les intérêts des sociétés qui les appliquent.

---

pour le droit commercial international (*Documents officiels de l'Assemblée générale, cinquante-huitième session, Supplément No. 17* et rectificatif (A/56/17 et Corr.3), annexe II).