Nations Unies E/CN.15/2009/2

Conseil économique et social

Distr.: Générale
3 février 2009

Original: Anglais

Commission pour la prévention et la justice pénale
Dix-huitième session
Vienne, 16-24 avril 2009
Points 3 a) et 4 de l'ordre du jour provisoire*
Débat thématique: "La fraude économique et la criminalité liée à l'identité"

Tendances de la criminalité dans le monde et mesures prises: intégration et coordination de l'action de l'Office des Nations Unies contre la drogue et le crime et des États Membres dans le domaine de la prévention du crime et de la justice pénale

Coopération internationale pour prévenir, poursuivre et réprimer la fraude économique et la criminalité liée à l'identité et mener des enquêtes sur ces infractions

Rapport du Secrétaire général

Table des matières

* E/CN.15/2009/1.

V.09-80494 (F)

I. Introduction

1. Dans sa résolution 2007/20, intitulée “Coopération internationale en matière de prévention, d’enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l’identité”, le Conseil économique et social a rappelé sa résolution 2004/26, dans laquelle il avait prié le Secrétaire général de convoquer un groupe intergouvernemental d’experts pour qu’il réalise une étude sur la fraude et sur l’abus et la falsification d’identité à des fins criminelles et de présenter un rapport sur les conclusions de l’étude à la Commission pour la prévention du crime et la justice pénale à sa quinzième session ou, le cas échéant, à sa seizième session, pour examen, s’est félicité du rapport du Secrétaire général sur les résultats de la deuxième réunion du Groupe intergouvernemental d’experts chargés de réaliser une étude sur la fraude et l’abus et la falsification d’identité à des fins criminelles (E/CN.15/2007/8 et Add. 1 à 3) qui avait été soumis à la Commission à sa seizième session et a encouragé les États Membres à examiner le rapport et, lorsque cela était approprié et conforme à leur droit interne, à la législation nationale, y compris pour ce qui est de la compétence, et aux instruments internationaux pertinents, à suivre les recommandations qu’il contenait pour élaborer des stratégies efficaces visant à répondre aux problèmes abordés dans le rapport, en ayant à l’esprit qu’une étude plus approfondie pourrait être utile.

2. Dans sa résolution 2007/20 également, le Conseil économique et social a encouragé les États Membres à envisager d’actualiser leur législation pour faire face à l’évolution récente de la fraude économique et à l’utilisation de technologies modernes pour commettre des fraudes transnationales ou massives ainsi qu’à tirer pleinement parti des technologies modernes pour prévenir et combattre la fraude économique et la criminalité liée à l’identité. Il a encouragé aussi les États Membres à envisager de conférer le caractère d’infraction criminelle à l’appropriation illicite, à la copie, à la fabrication et à l’usage impropre de documents ou d’informations d’identification, ou d’actualiser les infractions correspondantes, selon qu’il conviendrait.

3. Dans cette même résolution, le Conseil économique et social a encouragé les États Membres à prendre les mesures appropriées pour que leurs autorités judiciaires et leurs services de détection et de répression puissent coopérer plus efficacement dans la lutte contre la fraude et la criminalité liée à l’identité, si nécessaire en renforçant des mécanismes d’entraide judiciaire et d’extradition, compte tenu de la nature transnationale de ces infractions, et à tirer pleinement parti d’instruments juridiques internationaux pertinents, notamment de la Convention des Nations Unies contre la criminalité transnationale organisée[1] et de la Convention des Nations Unies contre la corruption;[2] il a également encouragé les États Membres à se concerter et à collaborer avec les entités commerciales et autres entités du secteur privé concernées, dans la mesure du possible, dans le but de mieux comprendre les phénomènes de la fraude économique et de la criminalité liée à l’identité et de coopérer plus efficacement dans la prévention, les enquêtes et les poursuites concernant ces infractions.

---

[1] Nations Unies, *Recueil des Traités*, vol. 2349, No. 42146

[2] Ibid., vol. 2225, No. 39574.

4. Dans sa résolution 2007/20, le Conseil économique et social a prié le Secrétaire général de rendre compte à la Commission pour la prévention du crime et la justice pénale, à sa dix-huitième session, de l'application de ladite résolution.

5. Le présent rapport contient un aperçu d'ensemble et une analyse des réponses reçues des États Membres concernant les efforts qu'ils ont déployés pour mettre en œuvre la résolution 2007/20 du Conseil économique et social et des informations qu'ils ont communiquées au sujet des politiques et des mesures qu'ils ont adoptées afin de promouvoir la prévention, les enquêtes, les poursuites et la répression de la fraude économique et de la criminalité liée à l'identité.

II. Aperçu d'ensemble et analyse des réponses reçues des États Membres

6. Les États Membres qui ont communiqué des informations et des documents pertinents sont les suivants : Allemagne, Arabie saoudite, Autriche, Azerbaïdjan, Bahreïn, Bélarus, Bulgarie, Canada, Égypte, Espagne, Estonie, Grèce, Japon, Jordanie, Koweït, Lettonie, Mexique, Maroc, Serbie, Tunisie, Ukraine et Uruguay.

Autriche

7. L'Autriche a relevé que la fraude économique et la criminalité liée à l'identité allaient de pair avec la corruption et que la mise en œuvre des dispositions correspondantes des chapitres III et IV de la Convention contre la corruption devrait par conséquent être appuyée par des mesures législatives appropriées au plan national et a souligné la nécessité de resserrer la coordination et la coopération internationales en vue de combattre efficacement ces formes de criminalité. Elle s'est référée à ce propos à une initiative qu'elle avait prise en 2004 pour créer le réseau européen de points de contact anticorruption (Partenaires européens contre la corruption), qu'elle présidait depuis sa création. L'Autriche a indiqué par ailleurs qu'en vue d'améliorer la coopération avec les milieux d'affaires et le secteur privé, les autorités nationales avaient organisé des manifestations annuelles, comme la "Journée autrichienne anticorruption" et des stages internationaux d'été, qui avaient fourni aux experts nationaux et internationaux une occasion d'échanger des données d'expérience et de discuter des divers aspects de la lutte contre la corruption.

Azerbaïdjan

8. L'Azerbaïdjan a mentionné les lois nationales qui criminalisaient de nombreuses infractions, dont la fraude, l'acquisition et la divulgation illégales de données protégées par le secret commercial ou bancaire, l'accès illégal à des données informatiques, la contrefaçon et la vente de documents officiels, de diplômes d'État, de sceaux, de tampons et de formulaires en blanc, l'usage de documents falsifiés et le vol de documents, et la destruction de documents, tampons et sceaux officiels. Ces dispositions étaient appliquées, lorsqu'il y avait lieu, conjointement avec d'autres dispositions de la législation nationale réprimant la corruption, le blanchiment d'argent, le transport illégal de migrants et la traite de personnes.

9. S'agissant de la coopération internationale, l'Azerbaïdjan a fait savoir qu'il avait conclu plusieurs accords bilatéraux et multilatéraux pour combattre la criminalité économique et participait à différents mécanismes et organisations régionaux comme l'Organisation économique de la mer Noire, la Communauté des États indépendants, le GUAM et l'Organisation de coopération économique. L'Azerbaïdjan était également partie à divers instruments internationaux pertinents, comme la Convention des Nations Unies contre la criminalité transnationale organisée et les protocoles y relatifs[3] et la Convention contre la corruption.

10. L'Azerbaïdjan a rendu compte également des mesures prises au plan national pour rassembler des données sur les tendances de la criminalité, et en particulier sur les délits liés à l'identité commis dans le but de faciliter l'entrée illégale de migrants ou de victimes de la traite des personnes su le territoire national. L'Azerbaïdjan a mentionné aussi les mesures adoptées pour garantir l'intégrité des systèmes d'information d'identification, notamment l'établissement de bases de données reliées entre elles et les efforts entrepris pour mettre en place, compte tenu de la pratique internationale, un système d'identification biométrique.

Bahreïn

11. Bahreïn a fourni des informations sur la législation promulguée pour combattre la criminalité économique, la fraude et le blanchiment d'argent. À cette fin, il avait notamment été créé au sein du Ministère de l'intérieur un service spécial chargé de la prévention de la délinquance économique.

Bélarus

12. Le Bélarus a indiqué qu'il avait été entrepris d'actualiser le code pénal à la lumière des tendances identifiées en matière de criminalité économique. Le code pénal, indépendamment de la répression de la fraude, criminaliserait également des infractions comme le vol au moyen de technologies informatiques, l'accès non autorisé à des informations stockées sur ordinateur ou l'altération de telles informations, le sabotage informatique, l'appropriation illicite d'informations stockées sur ordinateur, la fabrication ou la vente de dispositifs spécialement conçus pour avoir illégalement accès à des systèmes ou réseaux informatiques, l'élaboration, l'utilisation ou la diffusion de programmes nocifs et la violation des règles d'exploitation des systèmes ou réseaux informatiques. En outre, le code pénal considérait également comme des infractions les actes liés aux vols de passeports et d'autres documents personnels ainsi que l'acquisition illégale, la contrefaçon, la fabrication, l'utilisation ou la vente de documents officiels falsifiés.

13. Le Bélarus a souligné qu'il était partie à la Convention contre la criminalité organisée et à la Convention contre la corruption et qu'il coopérait avec les autres pays en matière d'extradition et d'entraide judiciaire sur la base de ces instruments. La coopération policière avec les autres États membres de la Communauté d'États indépendants était fondée sur le Programme intergouvernemental de mesures conjointes de lutte contre la criminalité approuvé en 2007. D'autres accords

[3] Ibid., vols. 2225, 2237, 2241 and 2326, No. 39574.

bilatéraux de coopération policière avaient été conclus avec la Fédération de Russie, la Lituanie, la République de Moldova et l'Ukraine. S'agissant de la criminalité économique et de la délinquance liée à l'identité, les services nationaux de répression coopéraient étroitement avec leurs homologues d'autres pays par l'entremise de l'Organisation internationale de police criminelle (INTERPOL) ainsi que sur la base d'accords bilatéraux. Le Bélarus a également mentionné les efforts entrepris pour resserrer la coopération avec les services d'investigation fiscale (financière) d'autres pays et a fourni des données statistiques concernant les cas de fraude, y compris de caractère transnational, qui avaient été enregistrés.

Bulgarie

14. La Bulgarie a donné un aperçu des dispositions du droit pénal national applicable à la fraude informatique et à la falsification de documents. Elle a signalé, à ce propos, qu'il avait été introduit en 2002 une nouvelle disposition pénale visant la fraude informatique, disposition qui avait été amendée en 2007. L'accès non autorisé à des données informatiques de quelque nature que ce soit, y compris l'information d'identification, était également réprimé. En outre, la législation pénale en vigueur réprimait l'établissement de documents officiels non véridiques ou la falsification du contenu d'un document officiel, le fait d'altérer des documents d'identification, des données personnelles ou les registres de l'état civil étant considéré comme circonstance aggravante.

15. La Bulgarie était partie à la Convention contre la criminalité organisée et aux protocoles y relatifs, à la Convention contre la corruption et à la Convention contre la cybercriminalité.[4] Les dispositions des articles 2 et 3 de la Convention contre la criminalité organisée avaient été pleinement appliquées. Dans la mesure où les infractions liées à l'abus et à la falsification d'identité à des fins criminelles constituaient des crimes graves au regard de la législation nationale et étaient réprimées conformément aux dispositions de la Convention contre la criminalité organisée, les dispositions de celle-ci leur étaient également applicables. En outre, la Bulgarie a fait savoir qu'elle était partie à la Convention européenne d'entraide judiciaire en matière pénale,[5] ainsi qu'à la Convention européenne d'extradition[6] et au Protocole additionnel[7] et au deuxième Protocole à cette Convention.[8] En outre, la Bulgarie avait intégré en droit interne la décision-cadre 2002/584/JHA du Conseil de l'Union européenne relative au mandat d'arrêt européen et aux procédures de remise entre États membres,[9] ainsi que l'Acte 2000/C 197/01 du Conseil de l'Union européenne établissant, conformément à l'article 34 du Traité relatif à l'Union européenne, la Convention d'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.[10] La Bulgarie avait par conséquent mis en place un cadre législatif très complet qui garantissait une coopération efficace en matière pénale, notamment dans des domaines comme les livraisons surveillées, les

[4] Conseil de l'Europe, *Série des Traités européens*, No. 185.
[5] Ibid., No. 30.
[6] Ibid., No. 24.
[7] Ibid., No. 86.
[8] Ibid., No. 98.
[9] *Journal officiel des communautés européennes*, L. 190, 18 juillet 2002.
[10] Ibid., C. 197, 12 juillet 2000.

échanges d'informations par vidéoconférence et l'établissement d'équipes d'enquête conjointes.

Canada

16. Le Canada s'est référé aux activités menées en matière de lutte contre la fraude économique et la criminalité liée à l'identité par la Commission pour la prévention du crime et la justice pénale et l'Office des Nations Unies contre la drogue et le crime (ONUDC), a rappelé que le Canada avait pris une part active à ces travaux et a fait savoir qu'étant donné la très large portée de la fraude économique et de la criminalité liée à l'identité, il fallait centrer l'attention sur des domaines prioritaires convenus. Le Canada a relevé à ce propos qu'une assistance devrait peut-être être fournie aux États Membres désireux d'actualiser la législation en vigueur en matière de fraude pour réprimer la fraude à grande échelle et d'autres formes nouvelles de fraude liées à la cyberdélinquance, notamment en leur communiquant les dernières informations disponibles sur les infractions visées, et qu'il fallait s'employer à aligner les normes et les pratiques nationales et internationales. Cela pouvait exiger l'élaboration de nouveaux instruments mais, pour maximiser les synergies et éviter les chevauchements inutiles, il y avait lieu d'utiliser dans tous les cas où cela a été possible les textes existants concernant la cyberdélinquance. En outre, le Canada a exprimé l'avis que les travaux futurs devraient s'attaquer au problème de plus en plus sérieux qu'était la délinquance liée à l'identité. Étant donné les travaux que menaient déjà les organisations gouvernementales et non gouvernementales dans ce domaine, il fallait assurer la coordination la plus étroite possible pour éviter les doubles emplois et les contradictions. De plus, la Commission pour la prévention du crime et la justice pénale et l'ONUDC devraient s'attacher surtout à fournir une assistance aux États Membres pour les aider à définir la criminalité liée à l'identité et les concepts connexes, à établir les infractions pénales appropriées et à adopter des mesures adéquates en matière de prévention du crime et d'aide aux victimes. Lorsqu'ils le pouvaient, les organismes des Nations Unies devaient également fournir une assistance aux autres institutions qui s'occupaient de formes spécifiques de documents d'identification, comme les passeports et les documents d'identification de caractère commercial, pour veiller à ce qu'il soit tenu compte des aspects touchant la prévention du crime et la justice pénale. Il fallait également, à cet égard, s'attacher en priorité à resserrer la coopération internationale en matière d'enquête et de poursuite des infractions et à promouvoir la coopération entre les institutions compétentes, y compris les entités commerciales et les États Membres, pour aider les victimes à réparer ou à recouvrer leur identité lorsqu'il en avait été abusé.

17. Le Canada, tout en convenant que les travaux futurs devraient surtout être axés sur le problème émergent de la délinquance liée à l'identité, a également mis en relief la corrélation étroite qui existait entre cette forme de criminalité et la fraude ainsi que sur le fait que le groupe intergouvernemental d'experts chargés d'entreprendre une étude sur la fraude et l'abus et la falsification d'identité avait recommandé de coordonner systématiquement les travaux accomplis dans ces deux domaines. Dans ce contexte, les travaux futurs devraient également tenir compte du fait qu'il pourrait être difficile, dans un avenir prévisible, d'établir une distinction entre la criminalité liée à l'identité et d'autres infractions connexes comme la

fraude, la criminalité liée aux migrations, les infractions en matières de passeports et autres documents de voyage ou d'identification et les infractions concernant l'abus de cartes de crédit et d'autres formes d'identification commerciale. S'il fallait mener partout dans le monde des recherches sur la nature et la portée de la criminalité liée à l'identité, le Canada a insisté sur le fait qu'il ne serait possible de rassembler des informations sur certains aspects du problème que lorsque les États Membres auraient élaboré des définitions spécifiques et criminalisé les infractions connexes dans leur législation nationale.

18. Le Canada a fait observer en outre qu'investir dans la formation, la recherche appliquée et la coopération entre le secteur public et privé pourrait avoir des dividendes substantiels en ce qui concerne la prévention et l'élimination de différentes formes de fraude et de criminalité liée à l'identité faisant intervenir des technologies de pointe. De plus, la disponibilité de technologies appropriées pourrait beaucoup améliorer l'efficacité des efforts de prévention ainsi que des enquêtes et des poursuites. Néanmoins, il fallait garder deux questions présentes à l'esprit. La première était que, pour combattre la cybercriminalité, y compris de nombreux types de fraude transnationale et de criminalité liée à l'identité, certains États devraient peut-être en aider d'autres à se doter des compétences techniques et des moyens de répression nécessaires pour pouvoir suivre efficacement les délinquants présumés et coopérer au plan international. La deuxième était qu'il fallait envisager et incorporer aux activités de coopération internationale des garanties de procédures appropriées et des mesures de protection des droits de l'homme. Le Canada a rendu compte de l'appui que les autorités canadiennes fournissaient continuellement dans les domaines de la formation, du développement technologique et de l'actualisation des législations concernant la cyberdélinquance, aussi bien au plan bilatéral que par l'entremise d'organisations intergouvernementales comme l'Organisation des Nations Unies, le Conseil de l'Europe, le Groupe des Huit, l'Association de coopération économique Asie-Pacifique, l'Organisation des États américains et le Commonwealth. Le Canada a rappelé qu'il avait pris une part active à la négociation de la Convention contre la cybercriminalité et était membre fondateur du réseau "24/7", qui reliait en temps réel les services de répression des États participants, au nombre desquels se trouvait le Canada. Le Canada a insisté sur le fait qu'il importait d'appuyer de telles initiatives et d'en améliorer l'efficacité.

19. Le Canada a souligné qu'étant donné la nature des systèmes d'identification, il fallait adopter une approche holistique en matière de prévention et de sécurité. Pour cela, il fallait, entre autres, examiner ou vérifier l'ensemble de l'infrastructure, y compris en ce qui concerne l'identification initiale des usagers et la délivrance et l'utilisation des documents. Passeport Canada était un exemple de cette approche globale. Passeport Canada s'était attaché non seulement à mieux sécuriser les passeports mais aussi à renforcer les mesures de lutte contre la fraude à l'étape de la délivrance des passeports en établissant une liste de contrôle des demandeurs, qui serait modernisée en 2009 et complétée par des techniques de reconnaissance faciale afin de dépister les personnes ayant présenté de multiples demandes sous des noms différents. Pour prévenir et détecter rapidement les vols d'identité, il fallait également former et alerter comme il convient le personnel des services chargés de la délivrance des passeports.

20. Le Canada s'est référé en outre au programme de prévention de la criminalité liée à l'identité à des moyens technologiques et aux mesures concrètes qui avaient été adoptées pour mettre en place de nouvelles précautions techniques contre la falsification, l'altération ou tout autre abus des pièces d'identité ou documents de voyage (élaboration de passeports électroniques). Il a également mis en relief l'importance de l'implication dans ces efforts du secteur privé, aussi bien en tant que producteur qu'en tant que bénéficiaire des mesures de sécurité et des techniques de prévention. Il a donné à ce propos des exemples des mesures adoptées par le secteur privé, et a mis en relief en particulier la collaboration des institutions financières et des fabricants de distributeurs automatiques de billets avec les services de répression en vue de contrer les nouvelles méthodes utilisées par des fraudeurs. Entre autres mesures de prévention, le gouvernement fédéral, les gouvernements des provinces et les entités commerciales et non gouvernementales intéressées utilisaient l'Internet pour sensibiliser le consommateur aux risques de fraude et de criminalité liée à l'identité.

21. Étant donné que la mondialisation du commerce, des transports et des technologies de l'information et des communications avait rendu encore plus nécessaire une coopération internationale dans les domaines liés à l'identification, à la prévention, aux enquêtes et à la répression des délits liés à l'identité, le Canada a expliqué qu'il était dans l'intérêt collectif de tous les États Membres de s'aider les uns les autres pour mettre au point des documents sécurisés et établir des institutions chargées de protéger l'intégrité de ces documents et des registres connexes lors de la délivrance et de leur utilisation. Cette assistance devait tendre à faciliter une vérification rapide et fiable de l'identité des nationaux et des résidents permanents. À ce propos, le Canada a également donné des informations sur la part active qu'il prenait aux travaux de différentes organisations internationales s'occupant de la sécurité des documents de voyage et de la gestion de l'identité, dont le Groupe consultatif technique sur les documents de voyage lisibles à la machine de l'Organisation de l'aviation civile internationale, son Groupe de travail sur les nouvelles technologies et son Groupe de travail sur le renforcement des capacités, le Groupe de travail antifraude des 5 nations et le Sous-groupe d'experts Rome/Lyon sur les migrations du G-8.

22. Le Canada était partie à la Convention sur la criminalité organisée. Tous les principaux types de fraude réprimés par la législation canadienne et la plupart des infractions existantes liées à l'identité étaient considérés comme des "crimes graves", conformément à l'article 2 b) de la Convention sur la criminalité organisée. Dans ce contexte, le Canada a souligné que la plupart des fraudes transnationales de grande envergure, et de loin, étaient le fait de groupes de criminels organisés et que les travaux futurs devraient par conséquent tendre à trouver le moyen d'utiliser plus efficacement la Convention sur la criminalité organisée plutôt que d'essayer d'élaborer de nouveaux instruments. S'agissant de la criminalité liée à l'identité, il serait peut-être nécessaire de rassembler davantage d'informations et de réaliser d'autres analyses avant de pouvoir parvenir à la même conclusion mais, d'une manière générale, le Canada considérait qu'il ne fallait élaborer de nouveaux instruments juridiques internationaux qui si, par exemple, cela s'avérait manifestement nécessaire pour réprimer des infractions spécifiques qui n'existaient pas déjà, faciliter l'adoption de mesures spécifiques en matière d'enquêtes ou de coopération internationale ou adopter des mesures pour aider les victimes, sur le plan international, à recouvrer ou à réparer leur identité, si ces questions n'étaient

pas couvertes comme il convient par les instruments juridiques internationaux existants. D'une manière générale, le Canada a insisté sur la nécessité d'aider les États Membres à actualiser leur législation concernant la fraude, à identifier les éléments à prendre en considération dans la qualification des niveaux d'infraction liés à l'identité et à utiliser les instruments juridiques internationaux existants.

23. Le Canada, sans être encore partie à la Convention relative à la cybercriminalité, avait déjà appliqué nombre des règles de cet instrument concernant les infractions à criminaliser, y compris différentes formes de cyberdélinquance comme la fraude informatique. Le Canada a exprimé l'avis que les dispositions générales de la Convention sur la cybercriminalité constituaient des modèles dont on pouvait utilement s'inspirer pour l'élaboration de nouvelles lois et pour la promotion de la coopération internationale dans ce domaine et que les États n'appartenant pas au continent européen devraient envisager soit d'adhérer à la Convention, soit de la prendre comme modèle pour formuler des lois nationales. Le Canada a ajouté que si l'ONUDC n'avait pas pour rôle ou pour mandat de promouvoir la Convention sur la cybercriminalité, il devrait collaborer aussi étroitement que possible avec l'organe du Conseil de l'Europe chargé de promouvoir sa ratification et sa mise en œuvre afin d'exploiter les synergies et d'éviter les contradictions.

24. Le Canada a également fourni des informations touchant les dispositions de sa législation nationale concernant les infractions comme la fraude à la consommation, la fraude commerciale, la cyberdélinquance, les infractions liées aux cartes de crédit et d'autres infractions connexes. Il a relevé à ce propos que la qualification des infractions liées à la fraude avait été revue en 2004 et que toutes les lois pénales étaient suivies de près de manière à identifier rapidement les nouvelles tendances et les nouveaux schémas de la criminalité et, en cas de besoin, à apporter les amendements requis à la législation en vigueur. Des ressources étaient allouées à la recherche pour rassembler des informations plus détaillées au sujet des tendances et des types de fraude et de l'ampleur du problème ainsi que d'autres informations afin d'évaluer l'efficacité de la législation existante et de déterminer si d'autres améliorations pourraient y être apportées. En ce qui concerne la criminalité liée à l'identité, en particulier, le Canada a déclaré qu'aucun comportement spécifique n'avait été criminalisé mais que, selon le cas, différentes dispositions existantes pouvaient être invoquées pour poursuivre de telles infractions, y compris les dispositions de caractère général réprimant des infractions comme le faux et l'usage de faux et des dispositions spécifiques touchant des infractions comme la falsification de documents d'identité déterminés, comme les cartes de crédit et les passeports canadiens. En outre, la législation nationale comportait des dispositions visant à combattre la cybercriminalité, notamment l'utilisation non autorisée d'ordinateurs, de réseaux, de données et de mots de passe, et elle réprimait l'imposture dans le but de commettre une fraude ou une infraction semblable. Par ailleurs, le Canada a fourni des informations sur les efforts déployés au plan national pour réviser le cadre juridique interne concernant la criminalité liée à l'identité. En novembre 2007, par exemple, le Gouvernement canadien avait déposé devant le Parlement des projets d'amendement au code pénal portant création de nouvelles infractions (vol d'identité et trafic d'informations d'identification) et modifiant les dispositions existantes pour combattre plus efficacement la criminalité liée à l'identité.

25. S'agissant de la rechersche et de l'analyse, le Canada a fait savoir que les autorités nationales rassemblaient et tenaient des données sur l'incidence de toutes les infractions, y compris les différentes formes de fraude, et sur les pourcentages d'affaires débouchant sur une condamnation. Il était prévu de réunir également des données concernant la criminalité liée à l'identité dès qu'entreraient en vigueur les amendements à la loi pertinente. Toutefois, accumuler suffisamment de données pour pouvoir évaluer l'incidence du phénomène et ses tendances prendrait sans doute un temps considérable. Indépendamment des évaluations périodiques des tendances de la fraude, il avait été organisé une enquête sur la fraude commerciale axée en particulier sur le commerce de détail, la banque et le secteur des assurances. Cette enquête avait pour but de faire mieux comprendre quelles étaient la nature et l'étendue des divers types de fraude commerciale au Canada ainsi que l'impact de la fraude économique sur les entreprises canadiennes. Les résultats de l'enquête devaient être publiés sous peu. En outre, il avait été réalisé des recherches académiques et il ressortait de l'une des études réalisées sur la base de réponses obtenues par l'Internet, publiée en 2008, qu'environ 6,5 pour cent de la population adulte du pays avait été victime, sous une forme ou sous une autre, d'une fraude à l'identité, la fraude la plus courante étant la fraude sur carte de crédit, qui représentait 60 pour cent des cas.

26. Le Canada a également insisté sur le fait qu'une coopération efficace devait s'instaurer entre le secteur privé, le système de justice pénale et les services de répression, aux échelons aussi bien national qu'international. Il a fait valoir à ce propos que si les principes du commerce et ceux de la justice pénale ne coïncidaient pas toujours, d'innombrables synergies pourraient être exploitées, surtout s'agissant de prévenir la fraude et la criminalité liée à l'identité. Des entreprises privées de secteurs clés comme la banque, la finance, les cartes de crédit, les technologies de l'information et de la communication et les voyages avaient également un rôle important à jouer. Il en allait de même des institutions académiques, les études menées par des spécialistes du droit commercial et du droit pénal ayant ouvert d'utiles perspectives et débouché sur l'organisation de différentes manifestations auxquelles avaient été représentées les positions des pouvoirs publics, des entreprises commerciales, des institutions académiques et d'autres parties prenantes (par exemple en matière de protection de la vie privée).

Égypte

27. L'Égypte a communiqué des informations concernant le cadre juridique applicable aux enquêtes et à la répression des délits économiques, dont le blanchiment d'argent, la corruption et la criminalité liée à l'identité. Le code de procédure pénale accordait au Ministère public une large compétence et de vastes pouvoirs pour combattre efficacement ce type de délit, y compris le pouvoir de vérifier des comptes bancaires pendant l'enquête et de demander la confiscation du produit de ces infractions. L'Égypte s'est également référée aux lois nationales portant création de tribunaux ad hoc pour connaître des affaires liées à la criminalité économique. Par ailleurs, un organe indépendant relevant de la Banque centrale avait été créé pour combattre le blanchiment d'argent et faciliter l'entraide judiciaire dans ce domaine. S'agissant de la coopération internationale en matière pénale, un service spécial du Ministère public avait été désigné autorité centrale chargée de

donner suite aux commissions rogatoires. Le fait que l'Égypte était partie à différents instruments juridiques internationaux dans ce domaine, y compris la Convention sur la criminalité organisée et la Convention contre la corruption, témoignait de sa ferme volonté de promouvoir cette coopération. L'Égypte a également mis en relief l'importance des activités de formation, qu'elles revêtent la forme de cours de formation interne du personnel ou d'une participation des magistrats du parquet aux programmes internationaux et régionaux de formation organisés par l'ONUDC et le Programme des Nations Unies pour le développement dans le cadre de son Programme sur la gouvernance dans la région arabe.

Estonie

28. L'Estonie a fait savoir que le code pénal contenait des dispositions réprimant la fraude, la contrefaçon et l'utilisation illicite d'informations d'identification en vue de faciliter la commission d'autres crimes. Elle a communiqué des informations concernant les efforts entrepris pour modifier le code pénal de manière à criminaliser le vol d'identité et a rappelé qu'elle était partie à la Convention sur la criminalité organisée et à la Convention sur la cybercriminalité.

Allemagne

29. L'Allemagne a souligné qu'elle attachait une grande importance à la lutte contre des infractions comme l'utilisation abusive ou frauduleuse de données personnelles et qu'il avait été élaboré des stratégies en vue de contrer les nouvelles menaces provenant de l'abus des systèmes informatiques dans les affaires et dans l'administration. Les éléments des infractions définies par la législation pénale en vigueur pouvaient être utilisés pour réprimer l'utilisation frauduleuse, l'altération ou la falsification de données liées à l'identité ou de données d'identification. Cependant, l'acte répréhensible n'était pas seulement celui consistant à obtenir frauduleusement des données personnelles mais plutôt celui consistant à utiliser frauduleusement les données ainsi obtenues. Le "phishing", par exemple, c'est-à-dire la tentative d'accéder à un compte bancaire en utilisant une fausse identité, pouvait faire intervenir des éléments d'infractions comme le vol de données, la fraude, la contrefaçon et la collecte et le traitement illicites de données.

30. L'Allemagne a signalé en outre qu'alors même qu'elle n'était pas encore partie à la Convention sur la cybercriminalité, des amendements avaient été apportés récemment à la législation pénale afin de combler les lacunes que celle-ci comportait et de l'aligner sur les dispositions de cette Convention. Les formalités nécessaires à la ratification de cette Convention se poursuivaient. De plus, bien que l'Allemagne n'ait pas encore ratifié la Convention contre la corruption, rien n'interdisait aux autorités nationales d'aider d'autres pays à faire enquête sur les cas de corruption et à combattre la corruption en général. Il était donné suite aux demandes d'extradition et d'entraide judiciaire conformément aux dispositions des traités et accords bilatéraux et multilatéraux auxquels l'Allemagne était partie ou de dispositions de ces instruments relatifs à l'assistance internationale en matière pénale.

31. L'Allemagne était partie à la Convention sur la criminalité organisée et à son Protocole additionnel visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants,[11] ainsi qu'au Protocole contre le trafic illicite de migrants par terre, air et mer, additionnel à cette même Convention.[12] Les accords ou arrangements conclus pour donner effet dans la pratique aux dispositions des articles 16 et 18 de la Convention sur la criminalité organisée pouvaient également être invoqués comme fondement juridique de la coopération internationale. L'efficacité au plan opérationnel de cette coopération avait été renforcée par l'établissement de contacts avec les homologues d'autres pays, notamment dans le contexte du Réseau judiciaire européen, ainsi que par des exercices de présentation de demandes d'entraide judiciaire et à l'utilisation du Rédacteur de requêtes d'entraide judiciaire élaboré par l'ONUDC.

Grèce

32. La Grèce a répondu que sa législation nationale contenait un très grand nombre de dispositions visant à combattre la fraude économique et la criminalité liée à l'identité. Pour une large part, ces dispositions étaient l'issue du processus d'intégration et d'adaptation du droit de l'Union européenne, y compris en ce qui concerne la protection des intérêts financiers des Communautés européennes. En outre, la fraude, la falsification de documents ou de fausses déclarations étaient au nombre des infractions visées par les dispositions réprimant l'implication d'une organisation criminelle dans la commission de crimes, qui était considérée comme une circonstance aggravante.

33. La Grèce a également fait savoir qu'elle était partie à la Convention pénale sur la corruption,[13] additionnelle au Protocole à la Convention pénale sur la corruption[14] et à la Convention contre la corruption. Dans ce dernier contexte, la Grèce avait participé au programme pilote d'examen de la mise en œuvre de la Convention et des experts et des représentants de l'ONUDC avaaient réalisé en mai 2008 une évaluation des mesures anticorruption avec l'aide des autorités nationales. La Grèce a signalé en outre qu'il avait été entrepris de promulguer une loi tendant à adapter au contexte national les dispositions de la Convention sur la criminalité organisée et de la Convention sur la cybercriminalité.

Japon

34. Le Japon a fait savoir que la fraude "furikome", fraude organisée qui consiste à utiliser des comptes bancaires et des téléphones cellulaires de tiers, avait causé de graves problèmes aux autorités japonaises.[15] Pour s'y attaquer, il avait été publié en juillet 2008 un plan d'action tendant à mener une action de sensibilisation et à promouvoir la coopération entre les institutions financières.

---

[11] Nations Unies, *Recueil des Traités*, vol. 2237, No. 39574.

[12] Ibid., vol. 2241, No. 39574.

[13] Conseil de l'Europe, *Série des Traités européens*, No. 173.

[14] Ibid., No. 191.

[15] Après s'être mis en rapport avec les victimes, habituellement au moyen d'un téléphone mobile plutôt que personnellement, les délinquants, par divers stratagèmes, amènent les victimes à virer de l'argent à un compte bancaire qu'ils désignent.

35. Le Japon a également mentionné que la législation nationale réprimait la fraude et la fraude informatique, y compris sous sa forme aggravée, lorsqu'elle était commise par un groupe. La loi prévoyait également l'exercice d'une compétence extraterritoriale pour la poursuite de ce type d'infractions. En ce qui concerne la criminalité liée à l'identité, la législation nationale non seulement réprimait les infractions classiques comme la contrefaçon et l'usage de faux, mais aussi d'autres actes comme l'utilisation illicite d'informations concernant les cartes de crédit, y compris la création, la possession ou l'acquisition illicites des informations électromagnétiques enregistrées sur une carte de crédit ou une carte bancaire et le fait d'obtenir frauduleusement, de vendre, d'acheter ou de posséder à des fins de revente des informations concernant les cartes de crédit. De plus, il devait être promulgué une nouvelle loi visant à améliorer la procédure applicable à la collecte d'éléments de preuve concernant les informations électromagnétiques et à autoriser la conservation d'informations touchant l'utilisation faite des services de communication.

36. S'agissant de la prévention, le Japon a signalé que la législation nationale imposait aux services de téléphonie mobile et aux magasins qui louaient des téléphones cellulaires des obligations rigoureuses en ce qui concerne l'identification de leurs clients. En outre, les services de répression avaient resserré leur collaboration avec les services de téléphonie mobile et les institutions financières et les avaient encouragés à adopter des mesures appropriées pour empêcher que des téléphones cellulaires et des comptes bancaires puissent être utilisés par des clients dont ils ne connaissaient pas l'identité.

37. Pour ce qui est de la coopération internationale, le Japon a fait savoir que la législation nationale concernant l'extradition et l'assistance internationale en matière d'enquêtes pouvait être invoquée comme fondement juridique de l'extradition et de l'entraide judiciaire. En outre, le Japon avait conclu plusieurs traités ou accords bilatéraux d'entraide judiciaire avec la Chine, les États-Unis et la République de Corée, et les négociations concernant la conclusion de traités semblables se poursuivaient avec d'autres pays. Le Japon n'avait pas encore ratifié la Convention sur la criminalité organisée et la Convention contre la corruption, mais les projets de loi d'application de ces deux instruments avaient été déposés devant le parlement pour approbation. Enfin, le Japon a fait savoir que ses services de répression coopéraient étroitement avec leurs homologues d'autres pays, notamment en échangeant des informations par l'entremise d'INTERPOL ou par la voie diplomatique.

Jordanie

38. Le Jordanie a répondu que des organes et institutions spécifiques avaient été créés pour faire enquête sur la criminalité économique et la cyberciriminalité ainsi que pour prévenir la fraude économique et encourager ainsi les investissements. Elle a signalé également que les autorités nationales coopéraient avec INTERPOL en échangeant des informations en vue de combattre la criminalité économique. Par ailleurs, des programmes de formation avaient été mis sur pied pour perfectionner les moyens et renforcer les capacités des autorités compétentes.

Koweït

39. Le Koweït a souligné que le code pénal réprimait les infractions liées à l'identité et qu'il avait été entrepris de revoir la législation en vigueur en matière de lutte contre le blanchiment d'argent afin de l'actualiser à la lumière de l'évolution des moyens utilisés. Il s'est déclaré résolu à promulguer de nouvelles lois et à combler les lacunes qui subsistaient dans le cadre juridique existant ainsi qu'à resserrer la coopération internationale en matière pénale aux échelons aussi bien bilatéral que régional. Dans ce contexte, il a signalé que des traités ou accords bilatéraux avaient été conclus avec un certain nombre d'États, dont Bahreïn, l'Inde, l'Iran (République islamique d'), l'Ouzbékistan, le Pakistan et la Turquie, et que les autorités nationales collaboraient avec leurs homologues d'autres pays pour négocier et conclure des traités semblables. Le Koweït était partie à la Convention sur la criminalité organisée et à la Convention contre la corruption.

Lettonie

40. La Lettonie a donné un aperçu de la législation nationale réprimant la fraude économique et la criminalité liée à l'identité. La législation en vigueur ne qualifiait pas spécifiquement certains actes de fraude économique mais contenait plusieurs dispositions réglementant des questions connexes. Ces dispositions criminalisaient une large gamme de comportements, dont la fraude et ses circonstances aggravantes (récidivisme et implication d'un groupe de criminels organisés), fraude informatique, fait de détruire, d'endommager ou de dissimuler intentionnellement des biens en vue d'obtenir une indemnité d'une compagnie d'assurance, commissions répétées de vols, fraudes et appropriations illicites à petite échelle, contrebande, contrefaçon, opérations d'initiés, blanchiment d'argent, non déclaration d'espèces, fraude à la consommation et violation des dispositions relatives à la documentation comptable et aux procédures régissant la compilation de comptes annuels ou de rapports statistiques.

41. Pour ce qui était de la criminalité liée à l'identité, la législation lettone contenait des dispositions réprimant la dissimulation de l'identité personnelle et l'utilisation de documents appartenant à un tiers ou d'un document d'identité falsifié. Le fait de commettre un tel acte dans le but d'éluder une responsabilité pénale ou de commettre une autre infraction constituait une circonstance aggravante. D'autres dispositions criminalisaient plusieurs types de comportement, comme l'imposture aux fins de l'acquisition de la citoyenneté, la falsification de documents et la délivrance intentionnelle ou l'utilisation de documents falsifiés par un agent public. La commission répétée de tels actes ou leur commission dans le but d'acquérir un avantage matériel constituait des circonstances aggravantes.

42. La Lettonie, qui était partie à la Convention sur la criminalité organisée, a fait savoir que la loi qui en avait incorporé les dispositions en droit interne était conforme aux dispositions des articles 2 et 3 de la Convention relatives aux infractions concernant la criminalité liée à l'identité et les autres infractions visées. La Lettonie était également partie à la Convention sur la cybercriminalité et au

Protocole additionnel à cette Convention relatif à la répression des actes de caractère raciste ou xénophobe commis au moyen de systèmes informatiques.[16]

43. En ce qui concerne la coopération internationale en matière pénale, le système juridique letton contenait des dispositions concernant l'extradition, l'entraide judiciaire, le transfert de procédures pénales et le transfèrement de condamnés. Le processus d'extradition, en particulier, était régi par la décision-cadre 2002/584/JHA du Conseil de l'Union européenne relative au mandat d'arrêt européen et aux procédures de remise entre États membres.

44. La Lettonie a rendu compte en outre des efforts entrepris pour adapter au contexte national la directive 95/46/CE du Parlement européen et du Conseil de l'Union européenne relative à la protection de l'individu en ce qui concerne le traitement des données personnelles et le libre mouvement de ces données.[17] Des amendements avaient été apportés à la législation en vigueur pour mettre pleinement en œuvre les dispositions de cette directive et définir les sanctions dont était passible leur violation.

Mexique

45. Le Mexique s'est référé à la législation nationale en vigueur concernant la prévention et la lutte contre le blanchiment d'argent et le financement du terrorisme, qui imposait un certain nombre d'obligations en ce qui concerne la validation et l'authentification de l'identité. Les institutions financières, en particulier, étaient tenues par la législation nationale de vérifier l'identité de leurs clients et d'identifier les transactions suspectes pour les signaler aux autorités compétentes. Le Mexique a fait savoir en outre qu'il était partie à la Convention sur la criminalité organisée et aux protocoles y relatifs et que la législation nationale continuait d'être alignée sur les dispositions de la Convention sur la cybercriminalité.

Maroc

46. La Maroc a communiqué des informations concernant la législation réprimant la cybercriminalité et les infractions liées à l'utilisation de systèmes automatisés de traitement des données. Il a souligné en outre que les dispositions de protection réglementant le commerce avaient été renforcées par l'introduction, en 2007, d'une loi sur l'échange électronique d'informations judiciaires. En outre, la législation nationale visant à combattre le blanchiment d'argent avait introduit une série de dispositions tendant à renforcer la coopération internationale dans ce domaine et il devait être créé prochainement un service de renseignement financier relevant directement du Premier Ministre.

47. Au plan institutionnel, le Maroc a fait savoir que sa Direction générale de la sécurité nationale s'employait à combattre la criminalité organisée sous toutes ses formes, y compris la criminalité liée à l'identité et la fraude économique. Les services nationaux de répression coopéraient activement avec leurs homologues d'autres pays, y compris par le biais d'échanges d'informations, de l'utilisation des

[16] Conseil de l'Europe, *Série des Traités européens*, No. 189.

[17] *Journal officiel des Communautés européennes*, L. 281, 23 novembre 1995.

mécanismes d'INTERPOL, de commissions rogatoires, de livraisons surveillées et, plus particulièrement de demandes d'identification d'empreintes digitales numériques. Afin de renforcer les capacités institutionnelles de combattre la fraude liée à l'abus d'identité, la police judiciaire nationale organisait des séminaires et des cours de formation.

48. S'agissant de la prévention de la criminalité liée à l'identité, le Maroc a signalé qu'il avait été introduit de nouvelles cartes d'identité nationales électroniques contenant des données biométriques qu'il était difficile de falsifier et qui visaient à renforcer la sécurité des documents d'identité et à éviter les fraudes auxquelles pouvait donner lieu leur abus. Des passeports biométriques devaient être introduits prochainement.

Arabie saoudite

49. L'Arabie saoudite a rendu compte des mesures prises au plan national pour faire enquête sur la criminalité économique et la poursuivre et la combattre efficacement. Dans ce contexte, elle a communiqué des informations concernant la loi bancaire et les mesures législatives adoptées pour criminaliser le blanchiment d'argent, la corruption active, la contrefaçon et la cyberdélinquance. Des stratégies et des plans de caractère plus général associant, entre autres, la société civile et le secteur privé avaient également été élaborés pour s'attaquer à la corruption. Ces stratégies prévoyaient également l'adoption de mesures de prévention axées principalement sur un effort de sensibilisation et d'appui aux centres de recherche. Pour améliorer la coordination des activités, l'on s'employait à élaborer des politiques multisectorielles associant différentes entités gouvernementales. L'Arabie saoudite a fait savoir qu'elle avait conclu une série d'accords bilatéraux et régionaux concernant la lutte contre la criminalité et qu'elle était partie à la Convention sur la criminalité organisée et a indiqué qu'elle avait aligné ses politiques de lutte contre le blanchiment d'argent sur les 40 recommandations du Groupe d'action financière sur le blanchiment de capitaux et que les autorités nationales avaient coopéré avec INTERPOL et le Groupe Egmont des cellules de renseignements financiers pour échanger des informations.

Serbie

50. La Serbie a donné un aperçu des dispositions du code pénal applicables à différentes infractions comme la fraude, la contrefaçon, la falsification de titres et de valeurs mobilières, le faux et l'usage de faux, l'abus des cartes de crédit, la falsification de documents de valeur, l'utilisation non autorisée de la raison sociale d'une autre société et les atteintes à la sécurité de données informatiques.

Espagne

51. L'Espagne a souligné que la législation nationale considérait la falsification de documents d'identité et l'utilisation de ces documents à des fins criminelles comme des infractions rattachées à des infractions pénales, comme le faux et l'usage de faux, visant à faciliter la commission d'infractions sous-jacentes, à savoir

l'"usurpation d'état civil". S'agissant de la fraude commise par le biais de l'Internet, l'Espagne a rendu compte des lois adoptées en matière de conservation des données concernant les communications électroniques et les réseaux publics de communication, conformément aux dispositions de la directive 2006/24/CE du Parlement européen et du Conseil de l'Union européenne relative à la conservation des données générées ou traitées dans le contexte de la prestation de services de communications électroniques d'accès public ou de réseaux publics de communication et portant modification de la Directive 2002/58/EC.[18] Aux termes des dispositions applicables, les opérateurs de services de télécommunication étaient tenus de conserver certaines données de sorte que la police puisse les utiliser aux fins de leurs enquêtes.

52. L'Espagne s'est référée à la collaboration qui s'était instaurée entre les autorités nationales compétentes et les entités privées du secteur financier, et en particulier les sociétés émettrices de cartes de crédit. Elle a fait savoir à ce propos que le Ministère de l'intérieur avait signé des accords de coopération avec des associations regroupant un grand nombre d'établissements de crédit et de compagnies d'assurance en vue de faciliter la prévention et la détection de la fraude. Ces accords avaient contribué à l'établissement de mécanismes de coopération utilisés pour obtenir des informations spécifiques sur des activités illicites et pour éviter la victimisation du consommateur. En outre, l'Espagne a indiqué que des consultations se poursuivaient avec des institutions financières du pays afin de mettre en place des mesures comme l'installation des systèmes d'alerte rapide et de contrôle nécessaires à la détection de documents d'identité falsifiés.

53. L'Espagne a déclaré par ailleurs que l'on utilisait les dernières technologies pour combattre la criminalité liée à l'identité essentiellement pour mieux sécuriser le processus de délivrance de pièces d'identité et de documents de voyage: il avait été décidé de mettre en place des systèmes d'identification biométrique et de promouvoir l'utilisation d'indicateurs physiologiques et comportementaux pour pouvoir procéder à des vérifications efficaces d'identité, et différentes initiatives avaient été lancées à cette fin conformément aux normes fixées par l'Organisation de l'aviation civile internationale et au Règlement No. 2252/2004 du Conseil de l'Union européenne établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. L'Espagne avait commencé à délivrer des cartes d'identité et des passeports électroniques en 2006.

54. En ce qui concerne la coopération internationale visant à combattre la fraude économique et la criminalité liée à l'identité, l'Espagne était partie à la Convention sur la criminalité organisée et à la Convention contre la corruption. Elle avait également conclu des traités et accords de coopération judiciaire et policière internationale. Les autorités espagnoles coopéraient avec INTERPOL et l'Office de police européen (Europol) et échangeaient des informations avec leurs homologues d'autres pays, y compris par le biais du Mécanisme de demande d'informations supplémentaires aux points d'entrée nationaux (SIRENE), qui faisaitt partie du système d'information de Schengen.

[18] *Journal officiel des Communautés européennes*, L. 105, 13 avril 2006.

Tunisie

55. La Tunisie a, par l'entremise de son Ministère de la justice, insisté sur le fait qu'il avait été mis en place une législation nationale pour combattre le blanchiment de capitaux et le financement du terrorisme. Aux termes de cette législation, les institutions financières, y compris les banques, étaient tenues de signaler aux autorités toutes les transactions et opérations suspectes. De plus, il avait été établi des normes rigoureuses de due diligence et les établissements financiers étaient tenus de connaître l'identité de leurs clients et de préserver les données concernant l'identité des personnes impliquées dans les transactions et la traçabilité des opérations financières. En outre, il avait été constitué un comité ad hoc chargé de réaliser des analyses financières des transactions suspectes et de promouvoir la coordination de l'action des différents départements et organismes compétents aux échelons aussi bien national qu'international ainsi que la participation des professionnels de la finance et d'autres domaines aux efforts visant à combattre le blanchiment d'argent.

56. De plus, la législation tunisienne contenait des dispositions réprimant une large gamme de crimes économiques et d'infractions liées à l'abus des technologies modernes dans le but de réaliser des activités illicites, dont la corruption, l'altération et la contrefaçon de sceaux et de pièces de monnaie, la banqueroute, la fraude et les autres comportements mensongers, l'enrichissement illicite, l'appropriation illicite, la copie, la fabrication et l'abus de documents d'information d'identification, la fabrication et l'utilisation de faux passeports et autres documents, l'accès non autorisé à un document informatique ou l'altération ou la destruction des données y figurant, la fabrication et l'utilisation de fausses cartes nationales d'identité et la falsification de passeports et de documents de voyage visant à faciliter l'entrée illégale ou la sortie d'une personne du territoire national. D'autres lois avaient été promulguées pour préserver la sécurité des systèmes informatiques.

57. En outre, les autorités tunisiennes avaient adopté des stratégies de partenariat et de collaboration avec le secteur privé afin de prévenir efficacement la criminalité liée à l'identité. À cette fin, il avait été mis en place des mécanismes chargés de superviser le crédit et de préserver la stabilité, l'intégrité et la sécurité du système financier et économique ainsi que de promouvoir la coopération avec les autorités chargées de la réglementation des secteurs financiers et de promouvoir des échanges d'informations. Par ailleurs, il avait été lancé des programmes afin de mieux faire comprendre les mécanismes et techniques utilisés pour faciliter le recyclage du produit d'activités criminelles, et en particulier des biens provenant de la fraude économique et de la criminalité liée à l'identité.

58. S'agissant de la coopération internationale en matière pénale, la Tunisie était partie à de nombreux traités et accords d'extradition et d'entraide judiciaire. Elle était aussi partie à la Convention sur la criminalité organisée, à la Convention contre la corruption et à la Convention internationale pour la répression du financement du terrorisme.[19] La Tunisie considérait le principe de reconnaissance mutuelle des décisions judiciaires comme l'un des piliers de la coopération internationale visant à combattre la criminalité économique.

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

59. Par l'entremise de son Ministère du commerce, la Tunisie a également souligné qu'elle s'était toujours employée à créer un climat favorable aux affaires. À cette fin, il avait été mis en place une infrastructure des communications et l'utilisation de moyens de communication modernes était encouragée dans le contexte de toutes les activités économiques, compte tenu de la nécessité de garantir la sécurité des usagers des technologies de l'information et de la communication et de celle de combattre l'utilisation illégale ou frauduleuse des réseaux informatiques.

60. Le cadre juridique tunisien concernant la fraude économique et la criminalité liée à l'identité dans le contexte des transactions commerciales, en particulier, contenait des dispositions tendant à protéger les droits de propriété industrielle et commerciale, le commerce et les échanges électroniques et le commerce international. S'agissant de la protection des marques de commerce, de fabrique et de services, l'on avait entrepris de préparer une législation nationale visant à donner effet aux conventions conclues sous les auspices de l'Organisation mondiale du commerce, et surtout l'accord relatif aux aspects des droits de propriété intellectuelle qui touchent au commerce.[20] Cet accord prévoyait la criminalisation de la contrefaçon des marques de commerce, de fabrique et de services et de toutes les activités connexes. En outre, il établissait, en tant que principe général, que cette violation, par contrefaçon, des droits du propriétaire de la marque donnait naissance à une responsabilité civile et pénale. En outre, cet accord criminalisait la livraison et la vente de marchandises portant une marque contrefaite. En octobre 2008, la Tunisie avait signé la Déclaration de Cannes contre la contrefaçon, qui tendait à combattre la contrefaçon de marques de commerce et de fabrique.

61. S'agissant du commerce et des échanges électroniques, la législation tunisienne contenait les dispositions visant à garantir que ces échanges soient réalisés de manière à promouvoir la sécurité et la confidentialité tout en prévenant toutes formes d'exploitation illicite. La législation tunisienne prévoyait également en matière d'échanges électroniques une série de garanties pour différents usagers et criminalisait un certain nombre de pratiques illicites.

62. En matière de commerce extérieur, la législation tunisienne garantissait la liberté des activités d'importation et d'exportation et comportait des règles visant essentiellement à protéger les intérêts des participants à l'activité économique et à combattre toutes les formes de fraude économique et de criminalité liée à la falsification d'identité, y compris en identifiant les personnes souhaitant procéder à des opérations d'importation et d'exportation comme désireuses de "participer au commerce extérieur".

63. S'agissant du cadre institutionnel lié aux transactions commerciales, la Tunisie a fourni des informations concernant les autorités tunisiennes compétentes et a donné un aperçu des mesures adoptées et des services fournis par ces autorités, dont la délivrance, l'annulation, la publication et l'administration de certifications électroniques; l'octroi d'autorisation d'agir en tant que "serveur de certifications électroniques" et le contrôle du respect de la loi; l'élaboration de spécifications techniques concernant les signatures électroniques; l'obligation pour tout usager d'un système de signature électronique d'informer le serveur de certifications

[20] Voir *Instruments juridiques reflétant les résultats du Cycle d'Uruguay de négociations commerciales multilatérales, Marrakech, 15 avril 1994* (Publication du secrétariat du GATT, No. de vente: GATT/1994-7).

électroniques de toute utilisation illicite de sa signature; l'obligation de faire enregistrer les signatures électroniques; l'imposition de différentes obligations au serveur de certifications électroniques, notamment celle de protéger le caractère confidentiel de l'information qui lui est confiée, de tenir un registre électronique des certificats de conformité, de suspendre la validité de tout certificat utilisé à des fins frauduleuses ou dont le contenu aurait été modifié; la délivrance de certificats de distributeurs Internet confirmant l'identité préservant la sécurité des sites commerciaux en vue de créer une relation fondée sur la confiance avec les clients en procédant à des achats électroniques par le biais d'un site Internet; et la délivrance d'un certificat de signature électronique identifiant l'auteur de la signature.

64. Par ailleurs, les autorités tunisiennes coopéraient avec les autorités de certification électronique étrangères grâce à la conclusion de traités et d'accords de reconnaissance mutuelle.

Ukraine

65. L'Ukraine a insisté sur le fait que ses autorités avaient consacré une attention spéciale à la prévention et à la détection de la fraude économique et de la criminalité liée à l'identité. En 2001, il avait été créé au sein du Ministère de l'intérieur, dans le cadre de la stratégie globale de lutte contre la criminalité économique, un service spécial chargé de lutter contre la cybercriminalité et les infractions aux droits de propriété intellectuelle. L'Ukraine a également fourni des informations sur la législation applicable à des questions connexes et a fait savoir que l'on constatait, de plus en plus, que la fraude économique était commise par "phishing" ou par pénétration des sites web des banques et des institutions financières en vue de voler des informations confidentielles. L'Ukraine a également signalé d'autres tendances, comme l'implication de membres du personnel des banques dans la commission des délits économiques, l'utilisation des systèmes de virements de fonds pour le blanchiment d'argent et l'utilisation de méthodes très pointues pour rassembler des informations sur les titulaires de cartes de crédit et d'autres informations confidentielles intégrées aux cartes de crédit.

66. En outre, l'Ukraine a signalé que l'incidence des délits liés à l'utilisation de cartes de paiement falsifiées avait quintuplé par rapport aux années précédentes. Dans plusieurs cas, les efforts intensifs menés par les autorités nationales pour détecter et poursuivre de telles infractions ou des délits semblables avaient été couronnés de succès.

Uruguay

67. L'Uruguay s'est référé aux dispositions de sa législation nationale concernant la contrefaçon et l'abus à des fins criminelles de documents comme cartes d'identité et passeports. L'Uruguay était partie à la Convention sur la criminalité organisée et à la Convention contre la corruption.

III. Conclusion

68. Les informations obtenues par le Secrétariat conformément à la résolution 2007/20 du Conseil économique et social confirment que les États Membres attachent une grande importance à la lutte contre la fraude économique et la criminalité liée à l'identité. Ces informations complètent celles, fournies par 46 États Membres, figurant dans le rapport du Secrétaire général sur les résultats de la deuxième réunion du Groupe intergouvernemental d'experts chargés de réaliser une étude sur la fraude, l'abus et la falsification d'identité à des fins criminelles (E/CN.15/2007/8 et Add. 1-3). Si les informations reflétées dans ledit rapport illustrent les problèmes que causent ces types de délits et les difficultés que rencontrent pour s'y attaquer les systèmes de justice pénale et les services de détection et de répression, celles qui figurent dans le présent rapport mettent en relief la nécessité d'élaborer soigneusement des stratégies détaillées et cohérentes pour mettre en œuvre dans différents domaines des interventions ciblées et bien préparées tendant à:

a) améliorer les législations, compte tenu des nouveaux besoins et des tendances émergentes;

b) mettre les institutions mieux à même de faire respecter les lois et de faire enquête sur les cas de fraude économique et de criminalité liée à l'identité;

c) resserrer la coopération internationale visant à combattre ces formes de délinquance;

d) élaborer et mettre en œuvre des politiques efficaces de prévention, notamment en ayant recours, selon qu'il convient, à de nouveaux moyens techniques de prévention;

e) établir des partenariats et exploiter les synergies entre les secteurs public et privé dans les domaines de la prévention, des enquêtes et des poursuites de ces types de crimes, compte tenu de la nécessité de sauvegarder comme il convient l'indépendance des fonctions d'enquête et de poursuites et des fonctions judiciaires;

f) promouvoir les activités de formation et d'assistance technique pour renforcer les capacités institutionnelles des autorités compétentes de faire face aux problèmes connexes.

69. La Commission pour la prévention du crime et la justice criminelle voudra peut-être étudier et recommander des moyens de continuer d'approfondir et d'enrichir le débat qui se poursuit au plan international au sujet des questions à l'examen. La discussion thématique concernant "La fraude économique et la criminalité liée à l'identité" qui doit avoir lieu à la dix-huitième session de la Commission constituera une occasion de poursuivre ce débat et pourra beaucoup contribuer à définir dans leurs grandes lignes les indications à suivre en ce qui concerne les initiatives les mieux appropriées devant être poursuivies en priorité à l'avenir.