



Conseil économique et social

Distr. générale
31 janvier 2011
Français
Original: anglais

Commission pour la prévention du crime et la justice pénale

Vingtième session

Vienne, 11-15 avril 2011

Point 6 de l'ordre du jour provisoire*

**Tendances de la criminalité dans le monde, et nouvelles questions
et mesures prises dans le domaine de la prévention
du crime et de la justice pénale**

Coopération internationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l'identité

Rapport du Secrétaire général

Résumé

Le présent rapport rend compte de la suite donnée par les États Membres à la résolution 2009/22 du Conseil économique et social et des politiques et mesures prises à l'échelle nationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la fraude économique et la criminalité liée à l'identité. Il renseigne également sur la manière dont l'Office des Nations Unies contre la drogue et le crime s'attache à promouvoir la compréhension mutuelle et l'échange de vues entre entités des secteurs public et privé sur les questions relatives à la fraude économique et à la criminalité liée à l'identité, en appuyant les travaux du groupe d'experts sur la criminalité liée à l'identité, dont il a assuré le service des réunions en 2010. Le présent rapport contient des informations sur l'assistance technique fournie dans le domaine de la lutte contre la criminalité liée à l'identité.

* E/CN.15/2011/1.



Table des matières

	<i>Page</i>
I. Introduction	3
II. Vue d'ensemble et analyse des informations communiquées par les États	5
III. Travaux du groupe restreint d'experts sur la criminalité liée à l'identité	21
IV. Matériel de formation technique sur la criminalité liée à l'identité	22
V. Conclusion	22

I. Introduction

1. Dans sa résolution 2009/22, le Conseil économique et social a pris note du rapport du Secrétaire général sur la coopération internationale pour prévenir, poursuivre et réprimer la fraude économique et la criminalité liée à l'identité et mener des enquêtes sur ces infractions (E/CN.15/2009/2 et Corr.1), qui renseignait sur les mesures que les États Membres qui avaient communiqué des informations avaient prises en application de la résolution 2007/20 du Conseil et sur leurs stratégies visant à répondre aux problèmes posés par ces formes de criminalité. Il a aussi pris note du débat thématique de la Commission pour la prévention du crime et la justice pénale, à sa dix-huitième session, sur "La fraude économique et la criminalité liée à l'identité". Le Conseil a salué les efforts déployés par l'Office des Nations Unies contre la drogue et le crime (UNODC) pour constituer, en consultation avec la Commission des Nations Unies pour le droit commercial international, un groupe restreint d'experts sur la criminalité liée à l'identité et réunir de manière régulière des représentants des gouvernements, des entités du secteur privé, des organisations internationales et régionales et des milieux universitaires pour mettre en commun des données d'expérience, élaborer des stratégies, faciliter la poursuite des travaux de recherche et convenir de mesures pratiques pour lutter contre la criminalité liée à l'identité. Il a pris note des travaux que le groupe restreint d'experts sur la criminalité liée à l'identité avait menés à ses réunions de Courmayeur (Italie), les 29 et 30 novembre 2007, et de Vienne, les 2 et 3 juin 2008 et du 20 au 22 janvier 2009.

2. Dans cette même résolution, le Conseil économique et social a encouragé les États Membres, compte tenu des recommandations 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 (E/CN.15/2007/8 et Add.1 à 3), convoqué conformément à sa résolution 2004/26:

a) À lutter contre la fraude économique et la criminalité liée à l'identité en s'assurant que les pouvoirs d'enquête étaient adéquats et, lorsqu'il y avait lieu, en révisant et en actualisant les lois s'y rapportant;

b) À mettre en place et à maintenir des moyens de répression et d'enquête adéquats pour se tenir au fait de l'évolution de la situation quant à l'exploitation des technologies de l'information, de la communication et du commerce dans la fraude économique et la criminalité liée à l'identité, notamment des sites Internet ou d'autres forums en ligne servant à faciliter le trafic d'informations d'identité ou de documents tels que passeports, permis de conduire et cartes nationales d'identité, et pour y faire face;

c) À envisager, au besoin, de créer de nouvelles infractions et d'adapter les infractions existantes face à l'évolution de la fraude économique et de la criminalité liée à l'identité, en gardant à l'esprit les avantages qu'il y avait à adopter des approches communes en matière d'incrimination, si possible, pour une coopération internationale efficace;

d) À renforcer la coopération internationale pour prévenir et combattre la fraude économique et la criminalité liée à l'identité, notamment en tirant pleinement parti des instruments juridiques internationaux pertinents;

e) À mettre au point une stratégie de collecte de données comparables sur la nature et l'ampleur de la criminalité liée à l'identité, notamment, si possible, du point de vue de la victime, qui permettrait la mise en commun de données entre les services de détection et de répression concernés et centraliserait, à l'échelle nationale, les données sur la nature et l'ampleur de la criminalité liée à l'identité, compte dûment tenu de la législation nationale;

f) À étudier, à l'échelle nationale, l'impact spécifique à court et à long terme de la fraude économique et de la criminalité liée à l'identité sur la société et sur les victimes de ces formes de criminalité et à élaborer des stratégies ou des programmes pour lutter contre ces formes de criminalité;

g) À adopter des pratiques utiles et des mécanismes efficaces pour aider et protéger les victimes de la fraude économique et de la criminalité liée à l'identité et, à cet effet, à favoriser une coopération efficace entre les entités des secteurs public et privé, par l'intermédiaire d'équipes d'intervention d'urgence ou d'autres mécanismes permettant d'apporter rapidement aux organismes publics et privés qui en ont besoin un soutien technique et des conseils en cas d'attaque électronique ou d'autres incidents mettant en jeu la sécurité des réseaux.

3. En outre, le Conseil économique et social a prié l'UNODC, en consultation avec les États Membres et compte tenu des organisations intergouvernementales compétentes et, conformément aux règles et procédures du Conseil, des experts d'établissements universitaires, d'organisations non gouvernementales concernées et du secteur privé, de collecter, d'élaborer et de diffuser:

a) Des documents et des lignes directrices sur la typologie de la criminalité liée à l'identité et sur les questions d'incrimination qui s'y rapportent pour aider les États Membres, sur demande, à créer de nouvelles infractions pénales liées à l'identité et à adapter les infractions existantes, compte tenu des travaux réalisés dans ce domaine par d'autres organisations intergouvernementales s'occupant de questions connexes;

b) Du matériel de formation technique, tel que des manuels, des recueils des pratiques utiles ou des lignes directrices, et d'autres ouvrages de référence scientifiques, criminologiques ou autres destinés aux agents des services de répression et aux organismes chargés des poursuites afin d'améliorer les connaissances techniques et les moyens dont ils disposent pour prévenir et combattre la fraude économique et la criminalité liée à l'identité;

c) Un recueil de pratiques utiles et de lignes directrices destiné à aider les États Membres à déterminer l'impact de ces infractions sur les victimes;

d) Un recueil de documents et de pratiques exemplaires sur les partenariats public-privé tendant à prévenir la fraude économique et la criminalité liée à l'identité.

4. Le Conseil économique et social a également prié l'UNODC d'apporter une assistance technique, y compris des conseils juridiques, sur demande, aux États Membres qui révisaient ou actualisaient leurs lois relatives à la fraude économique et à la criminalité liée à l'identité, afin qu'ils prennent les mesures législatives nécessaires, et de poursuivre ses efforts, en consultation avec la Commission des Nations Unies pour le droit commercial international, visant à promouvoir une compréhension mutuelle et un échange de vues entre les entités des secteurs public

et privé sur les questions se rapportant à la fraude économique et à la criminalité liée à l'identité, afin de faciliter la coopération entre les diverses parties prenantes des deux secteurs, par la poursuite des travaux du groupe restreint d'experts sur la criminalité liée à l'identité, dont la composition devrait respecter le principe de la répartition géographique équitable, et de faire régulièrement rapport à la Commission pour la prévention du crime et la justice pénale sur les résultats de ses travaux.

II. Vue d'ensemble et analyse des informations communiquées par les États

5. Les États Membres qui ont communiqué des informations et des documents concernant la suite donnée à la résolution 2009/22 du Conseil économique et social sont les suivants: Algérie, Allemagne, Arménie, Australie, Bélarus, Belgique, Bosnie-Herzégovine, Brunéi Darussalam, Canada, Chine, Chypre, Égypte, El Salvador, Fédération de Russie, Ghana, Guatemala, Japon, Jordanie, Maroc, Maurice, Mexique, Norvège, Panama, Pays-Bas, Philippines, Pologne, République de Moldova, République tchèque, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Serbie, Soudan, Suède, Suisse, Thaïlande, Togo, Trinité-et-Tobago et Ukraine.

Algérie

6. L'Algérie a signalé que sa législation incriminait l'usage de faux documents d'identité ou de faux justificatifs et la prise illégale d'intérêts. De plus, à l'occasion de récentes modifications du Code pénal, des infractions liées aux nouvelles technologies de l'information avaient été créées et les moyens d'investigation dont disposaient les services de détection et de répression pour identifier les auteurs d'infractions et recueillir les éléments de preuve nécessaires pour la procédure pénale avaient été renforcés. En 2004 avaient été créés, par modification du Code de procédure pénale, des pôles spécialisés constitués de magistrats auxquels des responsabilités et une compétence spécifiques étaient attribuées en matière de lutte contre le trafic de drogue, la criminalité transnationale organisée, l'atteinte aux systèmes de traitement automatisé de données, le blanchiment d'argent et le terrorisme. L'Algérie a précisé que la législation nationale contenait des dispositions relatives à l'entraide judiciaire et que les autorités du pays avaient conclu des accords bilatéraux d'entraide judiciaire et d'extradition.

Arménie

7. L'Arménie a mentionné les dispositions du Code pénal conférant le caractère d'infraction pénale à toute une série d'actes qui constituaient des délits économiques et qui relevaient de la fraude économique et de la criminalité liée à l'identité, ou qui supposaient le recours à l'informatique.

8. Elle a indiqué que sa loi sur les données à caractère personnel régissait les questions de gestion d'identité. Ce texte fixait les grands principes du traitement de ces données, les règles afférentes à la gestion de bases de données, les modalités d'accès à ces bases et les procédures à suivre pour porter plainte contre ceux qui traitaient de telles données dans le cadre de leur travail.

9. L'Arménie a aussi fait savoir que le Bureau du Procureur général avait enquêté sur plusieurs affaires de fraude et de blanchiment d'argent dont les auteurs présumés avaient dérobé de l'argent à des banques au moyen de fausses cartes de crédit ou avaient fait des achats au moyen de cartes de crédit fausses ou volées. Une intensification du recours à des documents d'identité falsifiés pour franchir les frontières avait été constatée.

Australie

10. L'Australie a signalé que, du fait que le pays était un État fédéral, les infractions de fraude visant une personne ou une entité autre que le Commonwealth (la fédération) étaient normalement du ressort des différents États et territoires; celles qui étaient traitées au niveau du Commonwealth concernaient généralement le Gouvernement fédéral. La fraude reposait habituellement sur les notions de tromperie et de malhonnêteté. L'Australie a fait référence aux dispositions du Code pénal qui visaient toute forme de recours à un réseau de télécommunications, à un ordinateur ou à Internet à des fins délictueuses.

11. L'Australie a indiqué que la sécurité des informations d'identité était cruciale pour la sécurité nationale, l'action de détection et de répression, la préservation des intérêts économiques et la sécurité des personnes; plusieurs États fédérés avaient d'ailleurs incriminé l'usurpation ou le vol d'identité. De plus, un projet de loi portant définition et incrimination de la criminalité liée à l'identité était en cours d'adoption, sur lequel tant le Commonwealth que les États fédérés pourraient s'appuyer. En vertu de cette loi, trois nouvelles infractions liées à l'identité seraient inscrites au Code pénal: la manipulation d'informations d'identité, la détention d'informations d'identité et la détention de matériel servant à fabriquer des documents d'identité. Le texte comprenait par ailleurs des dispositions qui permettraient aux victimes d'infractions liées à l'identité de demander une attestation décrivant la manière dont les informations les concernant avaient été utilisées.

12. S'agissant de la réponse apportée par la justice pénale, l'Australie a mentionné différentes opérations destinées à combattre la criminalité liée à l'identité, dont on estimait qu'elle constituait un domaine clef nécessitant une action renforcée à l'échelle nationale. Un rapport était en cours d'élaboration, qui ferait le point et renseignerait sur les activités menées dans ce domaine sur l'ensemble du territoire australien et mettrait en évidence les lacunes et points à améliorer pour la période 2010-2011.

13. S'agissant de prévention, l'Australie a signalé la mise en œuvre de la Stratégie nationale relative à la sécurité de l'identité, qui devait permettre de protéger l'identité de tous les citoyens australiens grâce au renforcement des processus nationaux de gestion d'identité, de manière à prévenir et combattre la criminalité liée à l'identité. De plus, des supports d'information avaient été publiés en vue de sensibiliser la population à la menace que représentait cette forme de criminalité, et un site Web (www.scamwatch.gov.au) avait été créé pour aider tout un chacun à reconnaître et signaler les escroqueries, y compris celles liées au vol d'identité. Par ailleurs, le secteur privé avait lui aussi mis au point des supports destinés à informer la population du danger que constituait cette forme de criminalité. Une coordination étroite était recherchée entre le Commonwealth, les États fédérés et le secteur privé, en particulier la banque et la finance.

14. L'Australie a souligné l'importance qu'il y avait à mener des travaux de recherche sur la criminalité liée à l'identité et à faire en sorte que des données plus exactes et complètes soient disponibles sur le sujet. L'office australien de la statistique avait ainsi réalisé une enquête auprès des ménages en 2007 et prévoyait d'en réaliser une autre à l'avenir.

Bélarus

15. Le Bélarus a évoqué les récents cas de fraude qui avaient été portés à la connaissance du Ministère de l'intérieur. Il a indiqué que les autorités nationales coopéraient avec celles d'autres États pour prévenir et combattre la fraude économique et la criminalité liée à l'identité. À cet égard, il a mentionné de récentes demandes d'assistance qui avaient été adressées aux services de détection et de répression compétents de Lettonie, de Fédération de Russie et d'Ukraine. La plupart de ces demandes avaient reçu une suite positive.

Belgique

16. La Belgique a communiqué des informations sur les efforts qu'elle déployait pour prévenir et combattre l'utilisation frauduleuse d'identité au moyen des technologies de l'information. La Federal Computer Crime Unit avait organisé des campagnes visant à sensibiliser les citoyens susceptibles d'être victimes d'infractions de ce type. Elle coopérait avec les autorités compétentes d'autres États et participait aux travaux de l'Anti-Phishing Working Group (Groupe de travail sur la lutte contre le hameçonnage) et de l'International Mass-Marketing Fraud Working Group (Groupe de travail international sur la fraude par marketing de masse), au sein desquels étaient échangées des informations devant permettre de rationaliser les efforts de lutte contre ce type de fraude. Afin de protéger les victimes, l'Union européenne envisageait l'élaboration d'une stratégie européenne de protection des données à caractère personnel dans le cadre du Programme de Stockholm pour la période 2010-2014¹, dans lequel le Conseil européen avait rappelé qu'il considérait comme une priorité la mise en place d'un espace de liberté, de sécurité et de justice. La Belgique a souligné que la fraude à l'identité était également considérée comme une priorité dans le Plan national de sécurité 2008-2011. Dans le but d'améliorer sa capacité à lutter contre la fraude à l'identité, elle prévoyait de renforcer la collaboration entre le gouvernement et les experts en faux documents.

Bosnie-Herzégovine

17. La Bosnie-Herzégovine a indiqué que ses lois pénales prévoyaient la sanction de tous les actes entamant la fiabilité de documents et fait référence à la législation nationale visant à protéger la confidentialité du traitement des données à caractère personnel. Une agence pour la protection des données à caractère personnel avait été créée; c'était une entité administrative indépendante chargée de surveiller le respect des lois relatives au traitement de ce type de données et de suivre l'évolution des besoins en matière de protection des données à caractère personnel.

18. La Bosnie-Herzégovine a fait savoir que ses services de justice et de répression compétents participaient activement à la lutte contre la fraude

¹ *Journal officiel de l'Union européenne*, 2010/C 115/01, 4 mai 2010.

économique et la criminalité liée à l'identité dans le cadre de l'action visant à combattre la criminalité organisée. Elle a mentionné les instruments internationaux sur le sujet auxquels elle était partie, à savoir la Convention des Nations Unies contre la criminalité transnationale organisée, la Convention des Nations Unies contre la corruption et la Convention sur la cybercriminalité du Conseil de l'Europe.

Brunéi Darussalam

19. Le Brunéi Darussalam a mentionné les mesures législatives qui avaient été prises pour incriminer et punir des actes tels que la falsification, l'accès non autorisé à des données informatisées et les opérations bancaires revêtant un aspect frauduleux. Il a décrit la législation nationale relative à la prévention du blanchiment d'argent et au financement du terrorisme, ainsi qu'à la confiscation du produit d'infractions autres que le trafic de drogue. Il a fait référence à la législation prévoyant la reconnaissance juridique des documents et signatures électroniques et les modalités des envois de fonds.

Canada

20. Le Canada a mis en avant le rôle moteur qu'il avait joué dans la réalisation, en 2007, d'une étude des Nations Unies sur la fraude et sur l'abus et la falsification d'identité à des fins criminelles, ajoutant qu'il continuait de participer activement aux activités de l'UNODC, notamment au sein du groupe restreint d'experts sur la criminalité liée à l'identité et dans le cadre de l'élaboration d'outils d'assistance technique en vue de l'incrimination directe ou indirecte de l'utilisation frauduleuse d'identité, d'améliorer l'efficacité de la Convention contre la criminalité organisée et d'autres instruments juridiques internationaux, de mettre au point des pratiques et directives utiles pour prévenir la criminalité liée à l'identité et pour soutenir et aider les victimes d'infractions de ce type.

21. Concernant la création de nouvelles infractions liées à l'identité, le Canada a souligné que, si chaque État pouvait certes définir ces infractions selon ses besoins propres compte tenu de la législation pénale en vigueur, il importait également que des approches communes soient adoptées de sorte que les différentes lois nationales permettent l'entraide judiciaire et d'autres formes de coopération.

22. Le Canada a rappelé qu'il avait été établi, dans l'étude de 2007 mentionnée au paragraphe 20 ci-dessus, qu'il existait un lien entre la disponibilité et l'utilisation des technologies de l'information et de la communication et la prévalence des infractions relevant de la fraude économique transnationale et de la criminalité liée à l'identité. Il a pris note du projet relatif à l'étude approfondie du phénomène de la cybercriminalité qui devait être réalisée en application de la résolution 65/230 de l'Assemblée générale, et a estimé que cette étude devrait examiner entre autres le rôle de la fraude économique et de la criminalité liée à l'identité à la fois comme motif et comme élément constitutif des infractions de cybercriminalité.

23. Le Canada a indiqué que l'élaboration de mesures adaptées pour apporter un soutien et une aide aux victimes de la criminalité liée à l'identité demeurerait problématique et que, de ce fait, les approches axées sur la victime étaient une composante essentielle de toute action globale prévoyant la mise au point de stratégies intégrées et pluridisciplinaires pour atténuer les préjudices dont les victimes continuaient de souffrir, prévenir la commission de nouvelles infractions

au moyen d'informations d'identité volées ou reproduites et aider les victimes à rétablir et corriger les informations falsifiées.

24. Le Canada a exposé les modifications qui avaient été apportées à la législation nationale pour incriminer le vol d'identité, le trafic d'informations d'identité et la détention frauduleuse ou le trafic de certains documents d'identité officiels et pour clarifier et étendre les actes érigés en infraction de manière à s'attaquer effectivement à la criminalité liée à l'identité. Il a évoqué le débat qu'avaient engagé en 2010 les services de détection et de répression et d'autres entités publiques compétentes concernant l'élaboration d'une stratégie nationale de lutte contre la criminalité liée à l'identité.

25. Le Canada a mis en avant les travaux que le Centre international pour la réforme du droit criminel et la politique en matière de justice pénale menaient sur la criminalité liée à l'identité et, plus particulièrement, les questions concernant les victimes. À cet égard, un manuel proposant des lignes directrices à l'intention des services de détection et de répression et des procureurs en matière de protection des victimes de la criminalité liée à l'identité était actuellement élaboré sous les auspices du groupe restreint d'experts de la criminalité liée à l'identité et en coopération avec lui.

Chine

26. La Chine a décrit les efforts déployés à l'échelle nationale pour modifier le Code pénal de sorte à permettre une coopération internationale renforcée dans la lutte contre la fraude économique et la criminalité liée à l'identité. Sur le plan opérationnel, les services de détection et de répression ciblaient les groupes criminels organisés impliqués dans ce type de fraude. Sur le plan judiciaire, des mesures avaient été prises en faveur de la mise en place d'un mécanisme efficace de poursuite et de sanction des auteurs d'infractions relevant de la criminalité économique. Sur le plan international, on s'était attaché à resserrer la coopération internationale en matière pénale, y compris pour l'extradition et le recouvrement d'avoirs. Par ailleurs, des campagnes avaient été menées à l'intention des agents publics, des organisations de la société civile, du secteur privé et de la population pour les sensibiliser et les informer quant aux conséquences de la fraude économique et de la criminalité liée à l'identité en termes de développement durable de l'économie.

Chypre

27. Chypre a signalé que, s'il n'existait pas de définition officielle de la criminalité économique à l'échelle nationale, toute activité illicite générant un produit au profit de son auteur était considérée comme relevant de la criminalité économique. Ces dernières années, quelques cas de fraude économique et de criminalité liée à l'identité avaient été constatés: escroqueries liées à des opérations bancaires électroniques (hameçonnage) et fraude liée au commerce électronique, mais aussi infractions faisant intervenir des cartes de crédit, des fausses déclarations, des fraudes, des contrefaçons et des actes commis à l'aide de l'informatique. Des actes de cybercriminalité avaient aussi été enregistrés: vol d'identité, atteinte à la confidentialité, à l'intégrité et à la disponibilité de données et systèmes informatiques et infractions liées à la pornographie mettant en scène des enfants.

28. Chypre a donné un aperçu des mesures préventives et répressives qu'elle avait prises face à la criminalité économique et indiqué que des services de répression spécialisés avaient été créés pour lutter contre la cybercriminalité et la criminalité économique. Les enquêtes sur les cas de fraude et d'infractions financières étaient la responsabilité du Groupe de la criminalité économique, qui coopérait étroitement avec différentes entités publiques et était aussi chargé de donner suite aux demandes d'assistance émanant d'autres États.

29. Pour ce qui était de la coopération internationale, Chypre a signalé que ses services de détection et de répression coopéraient étroitement avec des organisations internationales telles que l'Organisation internationale de police criminelle (INTERPOL) et l'Office européen de police (Europol). De plus, Chypre avait ratifié de nombreuses conventions internationales et signé plusieurs accords bilatéraux de coopération entre services de police ou autres services de l'État pour prévenir et combattre le terrorisme international, le trafic de drogue, la criminalité organisée et d'autres infractions graves. Dans la stratégie de prévention de la criminalité qu'elle avait adoptée en 2007, elle donnait la priorité au renforcement de la coopération avec d'autres pays européens, le Federal Bureau of Investigation des États-Unis d'Amérique, INTERPOL et Europol dans le domaine de l'échange d'informations et de la formation des agents de police.

30. Chypre a brossé un tableau général des bonnes pratiques suivies pour lutter contre la fraude économique et la criminalité liée à l'identité, dont l'organisation de conférences à l'intention des membres des différentes entités chargées des poursuites pénales, le recrutement de spécialistes, l'amélioration et l'intensification de la coordination et de la coopération interinstitutions avec différents États et organismes dans le domaine de l'échange d'informations et de la formation des agents de police, le renforcement des moyens administratifs dont disposaient les services de détection et de répression spécialisés, la création d'un bureau d'analyse criminelle équipé de techniques et logiciels appropriés, et la mise en place d'un système central informatisé de production de rapports sur les infractions graves et les infractions mineures.

République tchèque

31. La République tchèque a cité des dispositions de la législation nationale incriminant différentes formes de criminalité économique, dont la fraude, le blanchiment d'argent, l'accès non autorisé aux systèmes informatiques et supports de données, l'achat et la détention illégaux d'appareils et de mots de passe permettant d'accéder à des systèmes informatiques et à des données, l'endommagement par négligence du contenu de systèmes informatiques et supports de données, l'atteinte par négligence à l'intégrité de matériel informatique, la corruption, le trafic d'influence, la falsification et d'altération de documents officiels. Elle a communiqué des statistiques relatives aux poursuites et condamnations pour actes de criminalité économique et de criminalité liée à l'identité pour la période 2007-2010. Elle a aussi précisé les traités multilatéraux pertinents auxquels elle était partie.

32. Il a été fait mention des autorités tchèques chargées d'enquêter sur les cas de fraude et de criminalité liée à l'identité, dont faisaient partie les services de détection et de répression locaux et régionaux, ainsi que les services de police spécialisés. Il a été noté que l'Unité d'analyse financière du Ministère des finances,

qui était membre du réseau mondial des services de renseignement financier, avait pour fonctions de recevoir et d'analyser les signalements d'opérations suspectes; de remplir une mission de surveillance; de coordonner l'application des sanctions internationales au niveau national; de promouvoir la coopération internationale; de mener un travail législatif et fournir des orientations méthodologiques; et de mener des activités liées aux technologies de l'information et à la sécurité des services de renseignement financier. La République tchèque a donné un aperçu de ce que l'Unité d'analyse financière avait fait en 2008-2009, s'agissant notamment de sa participation aux travaux d'organisations internationales telles que le Conseil de l'Europe (dans le cadre de son Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (Comité Moneyval)), le Groupe Egmont, la Commission européenne (dans le cadre de son Comité sur la prévention du blanchiment de capitaux et du financement du terrorisme et de la plate-forme des centres de renseignement financier de l'Union européenne) et l'Organisation de coopération et de développement économiques. Les services nationaux de détection et de répression coopéraient également avec Europol dans la lutte contre la fraude économique et la cybercriminalité.

33. La République tchèque a décrit le travail de l'Agence de protection des données à caractère personnel, qui était chargée de surveiller le respect de la législation nationale en la matière. L'Agence coopérait avec ses homologues d'autres pays, avec les institutions de l'Union européenne et avec les organisations internationales actives dans le domaine. Comme suite à ses travaux, plusieurs modifications à la loi avaient été adoptées, notamment des règles strictes concernant la reproduction de cartes d'identité et de documents de voyage, et des règles afférentes à l'utilisation des numéros d'extraits d'actes de naissance. L'Agence participait à la lutte contre l'envoi massif de courrier électronique non sollicité (pourriel) et à la révision de la législation autorisant l'accès public à certaines données du registre des entreprises, ainsi qu'à la rédaction de nouveaux textes législatifs destinés à régir la collecte et l'utilisation de données d'ADN.

Égypte

34. L'Égypte a décrit sa législation nationale relative à la fraude économique et à la criminalité liée à l'identité, ainsi qu'aux organes chargés des affaires de ce type. Elle a indiqué s'être dotée de tribunaux spécialisés dans la lutte contre la criminalité économique et a exposé les mesures qui avaient été prises à l'échelle nationale pour garantir la sécurité et l'intégrité des données et documents d'identité. Elle a mentionné l'action préventive qui était menée, et qui prenait la forme notamment de l'élaboration de stratégies, de l'organisation d'activités de formation, de la conduite de campagnes de sensibilisation visant à faire mieux connaître l'évolution des infractions bancaires, et de la coopération avec les banques et les établissements financiers.

35. L'Égypte a aussi expliqué ce qu'elle faisait pour rationaliser les mécanismes de coopération internationale en matière pénale, en particulier par la ratification d'instruments multilatéraux et l'application de ceux auxquels elle était partie, la conclusion de traités bilatéraux, la promotion de l'échange d'informations et la coopération avec INTERPOL.

El Salvador

36. El Salvador a signalé la création au code pénal de plusieurs infractions liées à l'identité. Il a aussi indiqué que différentes modifications avaient été apportées à la législation pour permettre l'interception des télécommunications à titre temporaire dans le cadre d'enquêtes criminelles, sur décision du juge. En outre, les droits des témoins et des victimes étaient protégés par des dispositions juridiques spécifiques. El Salvador a donné des informations sur son nouveau code de procédure pénale, qui octroyait des pouvoirs élargis au procureur général en matière d'enquête et permettait la mise sur pied d'équipes d'enquête avec des partenaires étrangers.

Allemagne

37. L'Allemagne a fait observer qu'un certain nombre d'éléments constitutifs d'infraction en vertu de la loi pénale générale avaient trait à des actes tels que l'obtention à des fins frauduleuses de données à caractère personnel concernant des tiers, la falsification, la collecte et le traitement illégaux de données et l'altération de documents d'identité officiels. Elle a mentionné des statistiques concernant ce type d'affaires pénales et communiqué des informations sur les pouvoirs dont disposait la police judiciaire fédérale pour lutter contre la cybercriminalité dans le pays et sur le trafic de données d'identité numériques.

38. L'Allemagne a indiqué que les demandes d'extradition et d'entraide judiciaire pouvaient recevoir une suite favorable sur la base des accords bilatéraux et multilatéraux auxquels elle était partie et des dispositions de la législation nationale relatives à l'assistance internationale en matière pénale.

Ghana

39. Le Ghana a donné un aperçu des infractions économiques inscrites au code pénal. Il a fait savoir que l'organe national chargé de rédiger les lois s'efforçait d'élaborer de nouveaux textes visant les formes naissantes de criminalité économique et de cybercriminalité. Il a mis l'accent sur les formes particulières de fraude observées au Ghana et en Afrique de l'Ouest, comme l'escroquerie par demande d'avance d'argent et la fraude à la carte de crédit.

40. Le Ghana a expliqué quels problèmes il rencontrait dans la lutte contre la criminalité économique, précisant notamment qu'il devait former régulièrement les agents des services de détection et de répression et faire appel à davantage de spécialistes tels que des comptables, des juristes et des experts en technologies de l'information pour pouvoir s'attaquer efficacement aux nouvelles tendances de la criminalité économique. Il a décrit le cadre de la collaboration et de l'échange d'informations avec INTERPOL et proposé que cette collaboration soit renforcée à l'avenir.

Guatemala

41. Le Guatemala a donné des informations sur sa législation pénale visant la fraude économique et la criminalité liée à l'identité et a mentionné la mise en place de différents services spéciaux relevant du ministère public et chargés des affaires de criminalité économique et des infractions relatives à la propriété intellectuelle et aux avoirs volés. Il a exposé ce qui était fait pour garantir l'intégrité de la procédure

d'émission des passeports nationaux et les formations qui étaient offertes dans le domaine du contrôle des documents et de la prévention de la fraude.

Japon

42. Le Japon a décrit les efforts qu'il continuait de déployer pour réviser sa législation de manière à l'adapter à l'évolution des pratiques de fraude économique et de criminalité liée à l'identité. Ainsi, un texte de loi spécifique avait été adopté en 2006 puis modifié en 2008 pour combattre une forme de fraude dite "furikome", dont les auteurs avaient recours à des téléphones portables pour éviter d'être repérés par les autorités. Le Japon s'attachait à améliorer les procédures en place concernant le rassemblement de preuves en vue de réprimer les infractions faisant intervenir des schémas complexes de traitement de données informatiques.

43. Le Japon a indiqué que sa législation interne incriminait la fraude, y compris la fraude informatique, ainsi que la contrefaçon de documents, la production non autorisée de données électromagnétiques intégrées à des documents contrefaits, la détention de documents contrefaits contenant des données électromagnétiques non autorisées et l'obtention illégale d'informations relatives à des données électromagnétiques. Il s'employait à incriminer de nouveaux types d'actes tels que la création ou la diffusion de virus informatiques. Des dispositions juridiques simplifiées étaient entrées en vigueur, qui devaient permettre de mieux protéger les droits des victimes de la criminalité.

44. Le Japon a fait savoir qu'il pouvait, même en l'absence de traité applicable, apporter une assistance aux États qui en faisaient la demande ou extradier des personnes vers leur territoire sur la base de la législation nationale en vigueur. Cela étant, il avait conclu des accords d'extradition et d'entraide judiciaire avec différents États et avait signé la Convention contre la criminalité organisée et la Convention contre la corruption. La Diète avait approuvé la signature de ces deux conventions, mais la législation interne portant application de ces textes était encore en cours d'élaboration. Par ailleurs, la Police nationale japonaise favorisait la coopération, y compris l'échange d'informations, avec les services d'enquête étrangers par l'intermédiaire d'INTERPOL et par les voies diplomatiques, et elle avait constitué une base de données où figuraient notamment les noms des suspects et les moyens par lesquels les infractions étaient commises, afin d'enquêter sur la forme de fraude dite "furikome".

Jordanie

45. La Jordanie a exposé les mesures prises à l'échelle nationale pour mettre en place des institutions chargées de lutter contre la criminalité économique et la cybercriminalité. Elle s'attachait plus particulièrement à renforcer la coopération internationale en favorisant l'échange d'informations avec les services de détection et de répression étrangers. Des programmes de formation avaient été élaborés sur le sujet.

Maurice

46. Maurice a fait le point sur la législation nationale relative à la fraude économique et à la criminalité liée à l'identité. Elle a signalé que les autorités nationales s'appuyaient sur les instruments juridiques applicables pour réviser ou

actualiser les lois internes, compte tenu du fait que l'utilisation frauduleuse et la falsification de données d'identité étaient souvent associées à d'autres activités illicites telles que le blanchiment d'argent, la corruption et le terrorisme. Maurice a indiqué que, afin de maintenir des moyens de répression et d'enquête adéquats pour se tenir au fait de l'évolution de la situation quant à l'exploitation des technologies de l'information, de la communication et du commerce dans la fraude économique et afin d'y faire face, les forces nationales de police avaient massivement investi dans la formation et le matériel. Le pays s'efforçait d'intensifier la coopération internationale, notamment au moyen de l'application des dispositions de la Convention contre la criminalité organisée, ainsi que l'échange d'informations avec les États membres de la Communauté de développement de l'Afrique australe, l'Organisation de coopération régionale des chefs de police de l'Afrique australe et INTERPOL.

47. Maurice a signalé que les services de la Police nationale chargés des registres des infractions rassemblaient des données sur la nature et les conséquences de tous les types de criminalité, dont la criminalité liée à l'identité. Ces données étaient publiées chaque année et étaient généralement mises à la disposition des organisations qui en faisaient la demande à des fins d'analyse et de planification. Par ailleurs, l'Unité de renseignement financier était l'entité centrale qui, au plan national, recevait, analysait et diffusait auprès des services d'enquête et de surveillance les informations financières relatives au produit présumé d'infractions et aux infractions présumées de blanchiment d'argent, y compris aux activités ou opérations en lien avec le terrorisme. L'Unité était également responsable de l'échange d'informations avec les services de renseignement financier étrangers.

Mexique

48. Le Mexique a indiqué que son code pénal incriminait la fraude, y compris certaines formes spécifiques de fraude, mais non la fraude commise par Internet ou par d'autres moyens électroniques. En outre, plusieurs infractions apparentées à la fraude étaient visées par différentes lois financières. S'agissant de la protection des données à caractère personnel détenues par des entités publiques ou privées, la constitution avait été modifiée de telle sorte que cette protection soit reconnue comme un droit fondamental à part entière. Pour ce qui était des infractions en rapport avec le système financier, des instruments spéciaux d'enquête et de coopération avaient été mis en place, qui devaient permettre d'en repérer et poursuivre les auteurs. De plus, des mécanismes d'échange d'informations avec les établissements financiers avaient été institués.

49. Le Mexique a signalé avoir des difficultés à promouvoir la coopération entre les secteurs public et privé. Les problèmes tenaient aux fraudes financières massives, qui mettaient en évidence la nécessité de modifier les lois relatives aux infractions financières, et au manque de connaissances et de sensibilisation. Des actions de sensibilisation avaient été menées au moyen de réunions avec les services nationaux et étrangers compétents, comme le Ministère de la justice et la Commission des opérations de bourse des États-Unis. En outre, le Mexique a fait savoir qu'un inventaire comparatif des infractions financières commises au Canada, en Espagne, aux États-Unis, au Mexique et au Royaume-Uni avait été dressé.

50. Le Mexique était partie à la Convention contre la criminalité organisée et à la Convention contre la corruption, ainsi qu'à 14 instruments internationaux de lutte

contre le terrorisme, et il s'est dit intéressé par des sessions de formation sur l'incrimination et les enquêtes dans le cadre de son partenariat stratégique avec l'Union européenne.

Maroc

51. Le Maroc a mis en avant les problèmes que posent la fraude économique et la criminalité liée à l'identité, notamment la difficulté qu'il y a à élaborer une législation efficace contre ces infractions. Il a souligné qu'il s'agissait dans la plupart des cas de nouvelles formes de criminalité et que le Code pénal national, qui datait de 1962, n'avait pas été révisé pour leur donner la réponse voulue. En outre, le pays ne possédait aucun texte de loi sur les documents numériques, de sorte que les cartes d'identité et les passeports pouvaient facilement être falsifiés. Le Maroc a fait le point sur la législation existante en précisant que sa loi sur la lutte contre le terrorisme comprenait des dispositions sur la fraude à l'identité.

Pays-Bas

52. Les Pays-Bas ont indiqué que, ces dernières années, diverses mesures contre la criminalité financière et la fraude avaient été adoptées ou développées et que les organisations compétentes avaient vu leur rôle renforcé. Les instruments disponibles aux fins de la confiscation s'étaient multipliés et la lutte contre la fraude s'était considérablement intensifiée. Le pays a fourni des informations sur un projet d'enquêtes financières qui prévoit d'inclure ces dernières dans les activités de tous les services de détection et de répression. En outre, un programme axé sur l'application des mesures de lutte contre la fraude avait été mis en œuvre de 1998 à 2002. Dans leur rapport, les Pays-Bas ont mentionné un projet du Cabinet en matière de lutte contre la fraude et la criminalité financière (2002-2006) et un programme visant à renforcer les mesures de lutte contre la criminalité financière et économique (2007-2011) qui faisait partie d'un dispositif plus large mis en place pour améliorer la sécurité, intitulé "La sécurité commence par la prévention". Une description de ce dispositif a été fournie au Secrétariat séparément.

53. Les Pays-Bas ont déclaré qu'un projet de loi avait été présenté au Parlement, lequel prévoyait de renforcer les mesures d'enquête financière pour optimiser les chances de confisquer et de recouvrir des avoirs volés. S'agissant de la preuve de l'origine légitime du produit du crime, le projet édictait des présomptions légales qui pourraient s'appliquer aux avoirs acquis pendant une période pouvant remonter à six ans avant la commission de l'infraction pénale.

54. S'agissant de la fraude à l'identité, les Pays-Bas avaient lancé un programme visant à éviter les erreurs en la matière. Le programme concernait l'ensemble des organismes et institutions participant à la production ou au traitement d'informations et de documents d'identité et portait du principe que, pour être opérante, la chaîne de l'identité publique exigeait que soient assurées l'intégrité et la qualité de tous les processus, documents et bureaux d'enregistrement sous-jacents.

55. Les Pays-Bas ont indiqué que le Ministre de la justice du pays avait engagé des travaux de recherche juridique pour déterminer s'il était nécessaire et souhaitable que le droit pénal national traite la fraude à l'identité séparément des autres infractions existantes, telles que la contrefaçon. Un résumé de l'étude a été

soumis au Secrétariat. Sur la base des conclusions des travaux, les Pays-Bas étudiaient la possibilité d'ériger la fraude à l'identité en infraction à part entière.

Norvège

56. La Norvège a souligné l'existence d'une disposition juridique portant spécifiquement sur l'usurpation d'identité, approuvée par le Parlement en 2009. Contrairement aux dispositions générales sur la fraude, ladite disposition visait le fait de s'approprier illicitement l'identité d'une autre personne. Par ailleurs, le pays estimait que les conditions énoncées dans la Convention sur la cybercriminalité du Conseil de l'Europe avaient été pleinement incorporées dans le droit national.

57. La Norvège a évoqué les organismes spéciaux qui aidaient les forces de police nationales et internationales d'une part et les autorités de poursuite d'autre part à enquêter sur la fraude économique et la criminalité liée à l'identité et à poursuivre les auteurs de ces infractions de manière efficace. Le pays a noté qu'une stratégie nationale sur la cybersécurité avait été lancée en 2009 afin de recenser les mesures qui permettraient de protéger au mieux les systèmes informatiques stratégiques contre des incidents graves. Depuis 2010, les passeports nationaux contenaient des données biométriques, et la Norvège était en train de redoubler d'efforts pour créer des cartes nationales d'identité contenant des identifiants biométriques analogues.

58. La Norvège a également déclaré qu'une étude nationale sur l'usurpation et les abus d'identité avait été lancée en 2010. Pour montrer l'efficacité de la coopération entre les secteurs public et privé, le pays a mentionné l'existence du Centre norvégien pour la sécurité de l'information, qui concentrait ses efforts sur la sécurité de l'information et la lutte contre l'usurpation d'identité, entre autres, et qui était financé par le Gouvernement et par des acteurs privés, tels que des banques et des compagnies d'assurance.

Panama

59. Le Panama a présenté les activités des services judiciaires spécialisés créés en 2002 pour connaître des infractions à l'ordre économique et a fourni des informations sur l'incrimination en droit national de certaines infractions économiques et liées à l'identité. Le pays a par ailleurs décrit les mesures prises pour renforcer la sécurité des pièces d'identité, telles que l'établissement d'un système biométrique permettant la reconnaissance des empreintes digitales.

60. Le Panama a rendu compte des progrès réalisés dans le domaine des techniques d'enquête utilisées pour combattre les infractions concernées et a souligné la coopération entre les entités publiques et privées nationales. Il a indiqué qu'un système de vérification d'identité avait été créé pour servir spécialement la lutte contre la fraude à l'identité et a présenté les activités de sa Section de criminalistique informatique chargée de lutter, entre autres, contre la cybercriminalité, la fraude économique et la criminalité liée à l'identité. Au niveau international, le pays avait participé à des sessions de formation sur le blanchiment d'argent et d'autres infractions économiques.

Philippines

61. Les Philippines ont communiqué la liste des mesures adoptées par leur Conseil national de lutte contre le blanchiment d'argent pour combattre la fraude et la

criminalité liée à l'identité, notamment la possibilité de porter les affaires devant les tribunaux, la confiscation du produit du crime, la fourniture d'une aide aux victimes de ces infractions et l'organisation d'activités de sensibilisation.

Pologne

62. La Pologne a mis en avant l'adoption et la mise en œuvre d'une approche pluridimensionnelle de la lutte contre la fraude économique et la criminalité liée à l'identité. Dans ce contexte, elle avait adopté une législation adaptée pour sécuriser les informations stockées et transmises au moyen de systèmes électroniques. Le pays a dit effectuer des examens périodiques de la législation en vigueur.

63. Pour rendre plus efficace la lutte contre la fraude économique et la criminalité liée à l'identité, des unités spéciales avaient été créées au sein des bureaux des procureurs de la Pologne. Cette démarche avait permis d'améliorer l'efficacité des enquêtes et des poursuites, grâce à l'utilisation des dernières technologies de l'information et de la communication. De plus, une base de données électronique avait été constituée, qui autorisait la transmission rapide des données et la réalisation d'analyses concernant la typologie de la criminalité économique. Dans le cadre de la coopération internationale en matière de lutte contre la fraude économique et la criminalité liée à l'identité, le pays privilégiait la collaboration avec INTERPOL, Eurojust et le Réseau Judiciaire Européen.

64. La Pologne a communiqué des informations sur les activités de la Police nationale et sur les pouvoirs d'enquête des unités de police spécialisées chargées de lutter contre la criminalité économique et la cybercriminalité. Le Bureau de la coopération policière internationale de la Police nationale était chargé de la coopération internationale, de la formation et de l'échange d'informations, et apportait aussi des contributions à Europol en matière de fraude à la carte de crédit ("skimming"). La Police nationale coopérait avec le Ministère des finances, l'Autorité de supervision financière et le Service de renseignement financier, ainsi qu'avec l'Office européen de lutte antifraude pour protéger les intérêts financiers de l'Union européenne. Une coopération étroite entre les services nationaux de détection et de répression et les entités du secteur privé, telles que les banques et d'autres institutions financières, a été signalée.

République de Moldova

65. La République de Moldova a déclaré que le Ministère de l'intérieur avait organisé à l'intention du personnel concerné des sessions de formation sur la prévention et les méthodes efficaces pour révéler des infractions économiques, notamment celles relatives à l'utilisation de données personnelles, et sur le contenu d'un nouveau chapitre du Code pénal national portant sur la criminalité liée à l'information et la criminalité dans le domaine des télécommunications.

Fédération de Russie

66. La Fédération de Russie a souligné que, bien que la fraude soit mentionnée dans le chapitre du Code pénal national consacré aux infractions contre les biens dans le domaine des affaires, elle n'était pas considérée comme une infraction économique. Le pays a noté que les moyens utilisés pour commettre des fraudes pouvaient aussi jouer un rôle déterminant dans la commission d'autres infractions,

telles que la création et le développement illégaux d'entreprises, l'exercice illégal de l'activité bancaire, le blanchiment d'argent, l'obtention illégale de crédits, la contrefaçon de monnaie, de titres et de documents de paiement et la faillite fictive.

67. La Fédération de Russie a indiqué que l'identité était protégée par la Constitution et le droit fédéral sur les données personnelles et qu'une exploitation illicite des données personnelles tombait sous le coup du Code des infractions administratives. Cependant, le problème de la vulnérabilité de l'identité des personnes était aussi lié à la cybercriminalité, étant donné que la grande majorité des infractions relevant de la cybercriminalité impliquait l'obtention illicite d'une identité. S'efforçant d'élaborer des mesures efficaces de lutte contre la cybercriminalité, la Fédération de Russie avait ratifié un accord de la Communauté d'États indépendants sur la lutte contre la criminalité liée aux informations stockées sur ordinateur.

68. La Fédération de Russie a aussi déclaré que les autorités nationales travaillaient de manière coordonnée afin de combattre efficacement la criminalité économique. Le Ministère de l'intérieur avait mis en œuvre des mesures visant à renforcer la coopération avec les services de détection et de répression d'autres États dans le domaine de la lutte contre la criminalité économique et la criminalité liée à l'identité et à faciliter les recherches sur les nouvelles technologies de l'information, de la communication et du commerce favorisant la commission de telles infractions.

69. La Fédération de Russie a évoqué les traités internationaux, régionaux et bilatéraux qui servaient de fondements juridiques à la coopération internationale en matière de lutte contre la fraude économique et la criminalité liée à l'identité, entre autres infractions. Le pays a indiqué que le Bureau du Procureur général participait activement au renforcement des connaissances et de l'expertise dans le domaine de la coopération internationale en matière pénale.

Serbie

70. La Serbie a communiqué des informations sur sa législation nationale concernant la détection des infractions pénales à la sécurité des données informatiques, ainsi que des infractions à la propriété intellectuelle, des infractions sexuelles et des infractions à la paix publique et à l'ordre constitutionnel liées à l'utilisation de réseaux, systèmes et données informatiques, et concernant les poursuites et le jugement des auteurs de telles infractions. En outre, elle a fourni le libellé des dispositions du droit pénal relatives aux infractions suivantes: usurpation d'identité, fraude économique et utilisation illicite de cartes de crédit. Le pays a signalé la création de services spéciaux consacrés à la lutte contre la criminalité liée à l'usage des technologies de pointe au sein du Parquet et de la Cour supérieure.

Soudan

71. Le Soudan a déclaré qu'aucune infraction commise via l'Internet n'avait été signalée. Le pays a indiqué que des rapports sur la fraude économique, l'évasion fiscale et la contrefaçon de monnaies étrangères avaient été publiés et que les auteurs de telles infractions avaient été traduits devant les tribunaux. Il a mentionné les mécanismes institutionnels visant essentiellement à améliorer la détection du blanchiment d'argent et les enquêtes pénales en la matière.

Suède

72. La Suède a souligné que sa législation nationale autorisait les enquêtes sur la fraude économique et la criminalité liée à l'identité ainsi que la poursuite des auteurs de ces infractions. Les dispositions pénales sur la contrefaçon de documents originaux étaient en train d'être examinées afin qu'il soit tenu compte de l'évolution des technologies de l'information. En outre, l'autorité de poursuite nationale avait organisé des formations sur les questions pertinentes et produit différents rapports et lignes directrices. Des mesures avaient été prises pour améliorer le recueil et la qualité des données utiles et des statistiques sur la criminalité et pour renforcer l'appui aux victimes de fraude économique et de criminalité liée à l'identité. Le pays a insisté sur le fait qu'il était partie à plusieurs accords internationaux sur la coopération en matière pénale, lesquels étaient mis en œuvre via une législation nationale spécifique sur l'extradition, l'entraide judiciaire et la coopération internationale dans les procédures pénales et via l'exécution des décisions pénales.

Suisse

73. La Suisse a indiqué que sa législation nationale contenait des dispositions sur la corruption et le blanchiment d'argent, entre autres infractions. S'agissant de la confiscation du produit du crime, des mesures spécifiques avaient été adoptées pour étendre la compétence des autorités nationales. Le Code pénal avait été réformé dans les années 1990 pour traiter de la fraude économique et de la criminalité liée à l'identité et, à cet égard, les actes suivants avaient été érigés en infractions: attestation fausse, acquisition non autorisée de données, détérioration de données, utilisation frauduleuse d'un ordinateur et utilisation illicite de cartes de crédit et de chèques.

74. La Suisse a souligné qu'il existait différentes institutions chargées de contrôler le système de gestion de l'identité et que les informations sur la criminalité liée à l'identité étaient regroupées sur une page Web. Un institut de lutte contre la criminalité économique avait été créé en 2000 pour étudier l'impact de la criminalité économique sur la société et les victimes et pour élaborer une stratégie de lutte en la matière. Cette stratégie comprenait entre autres un volet consacré à la coopération entre les secteurs public et privé, qui était encouragée et appuyée.

75. La Suisse a déclaré être partie à toute une série d'instruments multilatéraux, notamment à la Convention des Nations Unies contre la criminalité organisée, à la Convention des Nations Unies contre la corruption et à 16 conventions et protocoles contre le terrorisme, ainsi qu'à tous les instruments du Conseil de l'Europe pertinents. En outre, le pays avait conclu des traités bilatéraux sur l'entraide judiciaire avec ses pays voisins, plusieurs États membres de l'Union européenne et des pays d'Europe du Sud-Est. Le Bureau de la police fédérale collaborait avec INTERPOL et Europol depuis 2006 et la Suisse était partie à l'Accord de Schengen et à la Convention d'application de l'Accord de Schengen depuis 2008.

Thaïlande

76. La Thaïlande a déclaré avoir amendé sa loi sur la lutte contre le blanchiment d'argent en 2009 pour tenir compte de l'apparition de la fraude économique et de la criminalité liée à l'identité. En outre, le Bureau de lutte contre le blanchiment

d'argent avait mis en place un projet à long terme pour mettre à jour la législation et la mettre en conformité avec les normes internationales en vigueur.

Togo

77. Le Togo a insisté sur le fait que, même s'il n'avait pas encore adopté de législation spécifique sur la fraude économique et la criminalité liée à l'identité, nombre des mesures législatives actuellement en vigueur s'appliquaient à ces infractions, notamment celles figurant dans le Code pénal national et dans d'autres instruments législatifs spécifiques. Le pays a déclaré avoir adopté un texte visant à faciliter la coopération régionale et internationale en matière pénale, notamment l'entraide judiciaire.

78. Le Togo a indiqué que des institutions compétentes en matière de détection des fraudes et d'enquête à cet égard avaient été créées. Par ailleurs, des systèmes numériques étaient utilisés pour la délivrance des permis de conduire et des cartes d'identité. Le Ministère de la sécurité avait créé un système de délivrance de passeports biométriques, et les mécanismes de contrôle aux frontières avaient été renforcés.

Trinité-et-Tobago

79. La Trinité-et-Tobago a indiqué que ses unités de police spécialisées dans la lutte contre la fraude et la corruption étaient les principales entités chargées d'enquêter sur la fraude économique et la criminalité liée à l'identité. L'aide d'INTERPOL et de l'autorité centrale du pays responsable des demandes de coopération internationale avait été sollicitée pour mener à bien les enquêtes extraterritoriales. Une autre unité, consacrée à la lutte contre la cybercriminalité, avait été créée en 2008 pour faciliter les enquêtes en ligne et la poursuite des auteurs de cyberinfractions.

80. La Trinité-et-Tobago a souligné que des activités de formation avaient été organisées en 2008 et 2009 à l'intention des enquêteurs et d'autres agents pour améliorer les compétences en matière de lutte contre la cybercriminalité, la fraude à l'assurance et la contrefaçon de monnaie, de comptabilité judiciaire, de techniques d'enquête et de criminalistique informatique. Le pays a cité les textes législatifs applicables et les amendements y afférents, qui incriminaient la fraude économique et la criminalité liée à l'identité et en vertu desquels certaines enquêtes et poursuites étaient menées.

Ukraine

81. L'Ukraine a noté que ses services de détection et de répression participaient à la lutte contre les infractions commises dans le domaine des affaires et contre la criminalité liée à l'identité, et a communiqué des statistiques pertinentes sur les mesures prises. Elle a indiqué qu'un grand nombre d'actes frauduleux avaient été commis via l'Internet, en s'appuyant en particulier sur des plates-formes commerciales telles que des sites d'enchères en ligne et de réseaux sociaux. Une progression régulière des transferts illicites de fonds via des pseudo-banques en ligne avait été observée.

82. L'Ukraine a fourni des informations sur les dispositions juridiques incriminant les infractions liées à l'identité et a présenté les procédures pénales engagées en 2010 par son Service de sécurité nationale. Elle a noté que le Ministère de l'intérieur avait élaboré un projet axé sur la lutte contre la criminalité, notamment la corruption, pour la période 2010-2015, qui devait avant tout permettre d'identifier les différentes formes de cybercriminalité et d'en poursuivre les auteurs.

Royaume-Uni de Grande-Bretagne et d'Irlande du Nord

83. Le Royaume-Uni a présenté sa stratégie nationale contre la fraude, qui comprenait un examen stratégique des mesures nationales visant à combattre la criminalité liée à l'identité. Cet examen avait permis de mieux comprendre les problèmes posés par cette forme de criminalité ainsi que les grandes priorités dont il faudrait tenir compte à l'avenir, lors de l'adoption de mesures de lutte contre les infractions visées. Une équipe spéciale de la lutte contre la criminalité liée à l'identité, réunissant organisations des secteurs privé et public et organismes de détection et de répression, avait été créée pour combattre cette forme de criminalité de manière plus intégrée.

84. Le Royaume-Uni a souligné que, dans le cadre d'un programme plus vaste d'activités pluri-institutions visant à lutter contre la criminalité liée à l'identité, des travaux très importants avaient été menés, parmi lesquels: le lancement d'une stratégie de protection de l'identité; l'évaluation du résultat des opérations récentes visant à faire échec aux auteurs d'infractions liées à l'identité, qui avait permis d'améliorer le partage des informations et d'identifier les principaux criminels et groupes criminels organisés; et le développement des activités de la Police de Londres contre la fourniture de matériel d'impression professionnel susceptible d'être utilisé dans la fabrication de fausses pièces d'identité.

III. Travaux du groupe restreint d'experts sur la criminalité liée à l'identité

85. Sur la base de la pratique constamment suivie depuis 2007 et conformément à la résolution 2009/22 du Conseil économique et social, en 2010, l'UNODC a tenu deux réunions du groupe restreint d'experts sur la criminalité liée à l'identité à Vienne, la première du 18 au 22 janvier et la seconde du 6 au 8 décembre. Ces réunions reposaient sur une approche multipartite, l'objectif étant de permettre aux représentants des États Membres, du secteur privé, des organisations internationales et des milieux universitaires de se retrouver et de mettre en commun des données d'expérience, d'élaborer des stratégies, de faciliter la poursuite des travaux de recherche et de convenir de mesures pratiques pour lutter contre la criminalité liée à l'identité. Les rapports de ces réunions ont été présentés à la Commission pour la prévention du crime et la justice pénale sous forme de documents de séance (<http://www.unodc.org/unodc/en/organized-crime/index.html>), à titre d'information.

86. Lors des réunions susmentionnées, le groupe restreint d'experts sur la criminalité liée à l'identité a eu l'occasion d'examiner les supports que l'UNODC avait mis au point en application de ses recommandations et des mandats prévus dans certaines résolutions du Conseil économique et social, et de donner ses impressions. Ces supports abordaient principalement les questions de droit, de

justice pénale et de politique générale relatives à la criminalité liée à l'identité, notamment la typologie de cette criminalité et les approches de l'incrimination, la coopération internationale, la protection des victimes et les synergies possibles entre les secteurs public et privé, en particulier dans le domaine de la prévention. Par ailleurs, le groupe restreint d'experts a engagé des discussions approfondies et ciblées sur le recours à la criminalistique pour combattre et prévenir la criminalité liée à l'identité et sur les moyens les plus efficaces de protéger les droits des victimes. Il a servi de cadre pour l'analyse comparative du problème de ladite criminalité et la présentation d'une vue d'ensemble des diverses approches adoptées pour y répondre dans différentes régions.

IV. Matériel de formation technique sur la criminalité liée à l'identité

87. Conformément aux conclusions et aux recommandations formulées lors des réunions du groupe restreint d'experts sur la criminalité liée à l'identité, l'UNODC s'attache à promouvoir de nouveaux travaux de recherche et à élaborer du matériel de formation sur la criminalité liée à l'identité. Dans un manuel consacré à ce sujet qui doit paraître et être diffusé aux États Membres prochainement, l'UNODC présentera une série d'options et d'éléments à prendre en compte lors du traitement de questions relatives à la justice pénale nationale (tels que la typologie de la criminalité, les diverses approches de l'incrimination et la protection des victimes), ainsi que les difficultés particulières liées à la promotion de la coopération internationale en matière pénale et les synergies et partenariats possibles entre les secteurs public et privé, notamment pour ce qui est de la prévention de la criminalité liée à l'identité. Le manuel comprendra des travaux de recherche et des matériels didactiques, notamment sur le recours à la coopération internationale pour lutter contre ladite criminalité.

88. Le manuel sur la criminalité liée à l'identité susmentionné est destiné aux législateurs, décideurs, procureurs, services de détection et de répression et praticiens, ainsi qu'à d'autres parties prenantes (telles qu'aux représentants de certaines organisations internationales et intergouvernementales, du secteur privé et des milieux universitaires). On prévoit aussi de l'utiliser à des fins didactiques dans les programmes d'assistance technique et les activités de renforcement des capacités pour parfaire les connaissances spécialisées dont on dispose sur les moyens de traiter les problèmes juridiques, institutionnels et opérationnels relatifs à la nouvelle forme de criminalité qu'est la criminalité liée à l'identité.

V. Conclusion

89. La Commission pour la prévention du crime et la justice pénale voudra peut-être tenir compte des informations fournies par les États Membres sur les efforts déployés au niveau national pour mettre en œuvre des mesures et des politiques visant à prévenir la fraude économique et la criminalité liée à l'identité, à mener des enquêtes sur les infractions concernées et à en poursuivre et en punir les auteurs. Ce faisant, elle pourrait donner de nouvelles orientations à l'UNODC sur la fourniture d'une assistance technique aux États Membres qui en font la demande,

destinée à aider ces derniers à adopter des mesures législatives appropriées pour lutter contre lesdites infractions, à élaborer et à appliquer de solides mécanismes d'enquête et de détection et de répression, à adopter les meilleures pratiques et des dispositifs efficaces de protection des victimes et à garantir une coopération internationale efficace et rapide pour limiter la commission desdites infractions. La Commission voudra peut-être examiner les travaux du groupe restreint d'experts sur la criminalité liée à l'identité lorsqu'elle se penchera sur les éléments d'une approche pluridisciplinaire pour prévenir et combattre la criminalité liée à l'identité.
