Nations Unies E/CN.15/2007/8/Add.3

Conseil économique et social

Distr.: Générale
31 janvier 2007

Français
Original: Anglais

Commission pour la prévention du crime et la justice pénale
Seizième session
Vienne, 23-27 avril 2007
Point 4 de l'ordre du jour provisoire*
Criminalité dans le monde: tendances et réponses: combinaison et coordination des efforts de l'Office des Nations Unies contre la drogue et le crime et de ceux des États Membres dans le domaine de la prévention du crime et de la justice pénale

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

Rapport du Secrétaire général

Additif

Criminalité liée à l'identité

Table des matières

* E/CN.15/2007/1.

V.07-80502 (F) 290307 300307

I. Introduction

A. Nature de la criminalité liée à l'identité

1. La possibilité d'identifier précisément chaque individu[1] est un élément fondamental de l'activité sociale, politique et économique sous pratiquement tous ses aspects. Une identité doit être créée et rattachée à l'entité spécifique qu'elle identifie. Par ailleurs, il faut créer, transmettre, stocker et extraire des informations d'identification qui sont généralement reliées à d'autres données sur l'individu en question, telles que sa nationalité ou sa citoyenneté, ses documents financiers et bancaires et ses antécédents judiciaires, ainsi qu'à des informations personnelles ou commerciales analogues. Le rôle fondamental que joue l'identité dans des systèmes à la fois très nombreux et différents, ouvre la voie à un large éventail de possibilités d'infractions, à partir du moment où des informations d'identification de base peuvent être modifiées ou falsifiées et que les systèmes destinés à créer, modifier, extraire et vérifier l'identité et d'autres informations peuvent être corrompus. C'est pourquoi presque tous les États traitent d'une manière ou d'une autre des questions liées à l'identité dans le cadre de leurs systèmes de justice pénale et de droit pénal.

2. À l'heure actuelle, la plupart des États se contentent de traiter le problème de l'identité au niveau législatif et décisionnel du point de vue des infractions susceptibles d'être commises par abus d'identité. Cependant, depuis peu, certains États commencent à l'aborder du point de vue de l'identité elle-même. On considère qu'en plus de l'usage impropre de l'identité, le fait de faciliter, de préparer ou de favoriser un tel acte (par exemple d'usurper, de copier ou de créer de toutes pièces une identité ainsi que d'altérer de différentes manières un système d'identification) devrait être considéré comme une nouvelle forme distincte d'infraction pénale. Cela concorde avec d'autres évolutions récentes, comme en témoigne notamment la Convention des Nations Unies contre la criminalité transnationale organisée (résolution 55/25 de l'Assemblée générale, annexe I) et la Convention du Conseil de l'Europe sur la cybercriminalité[2]. En incriminant les infractions liées à l'identité, on reconnaît que l'infraction principale de l'abus d'identité peut entraîner une série d'infractions accessoires et l'on permet ainsi au système de justice pénale d'intervenir plus tôt. Cette approche reflète aussi l'idée selon laquelle, lorsque l'identité authentique d'un individu est utilisée pour commettre d'autres infractions, ledit individu, de même que les personnes touchées par les infractions ultérieures,

---

[1] On avait donné aux États une description de la fraude à l'identité qui englobait des faits visant les informations relatives à l'identité ou à l'identification des personnes tant physiques que morales, mais on ne leur a pas posé de questions spécifiques sur l'identité des personnes morales. Dans leurs réponses, plusieurs États ont mentionné des registres d'entreprises ou des systèmes analogues servant à établir l'identité des personnes morales; mais les informations communiquées n'étaient pas suffisantes pour évaluer les problèmes particuliers associés à l'identification des personnes morales.

[2] Voir, par exemple, l'article 5 de la Convention contre la criminalité organisée sur l'incrimination de la participation à un groupe criminel organisé et l'article 8 de la Convention sur la cybercriminalité (Conseil de l'Europe, *Série des Traités européens*, n° 185) qui dispose que l'on doit ériger en infraction pénale le fait intentionnel de commettre une fraude informatique, que cette dernière aboutisse ou non. Ces deux conventions prévoient des dispositions qui traitent largement de la nécessité de lutter contre les actes visant à faciliter, préparer et favoriser de telles pratiques.

subissent des préjudices et devraient être considérés comme des victimes. L'incrimination des infractions liées à l'identité, notamment lorsque des groupes criminels organisés sont impliqués, illustre en outre la reconnaissance du fait que les documents et les informations d'identification sont devenus une marchandise illicite qui est transférée des auteurs de ces infractions à d'autres personnes qui commettent de nouvelles infractions en utilisant ces informations ou les fausses identités ainsi créées.

B. Terminologie employée dans le présent rapport

3. Dans sa résolution 2004/26, le Conseil économique et social a prié le Secrétaire général de convoquer un groupe d'experts pour qu'il réalise une étude sur "la fraude et l'abus et la falsification d'identité à des fins criminelles" ainsi que les infractions connexes. Lors de leurs premières délibérations, telles que les reflète le questionnaire destiné à recueillir des informations, les experts n'ont pas examiné le sens précis de chacun de ces termes ni cherché à faire une distinction entre la fraude à l'identité et l'usurpation d'identité. Seul un État a donné une définition législative, la majorité ayant simplement indiqué que la description proposée dans le questionnaire (E/CN.15/2005/CRP.5, question 33) reflétait avec justesse les problèmes qu'ils avaient rencontrés. Les experts avaient décidé à titre préliminaire et sans parti pris d'employer le terme "identity fraud" (fraude à l'identité), mais il est ressorti des réponses des États et d'autres documents que certaines infractions signalées se rapprochaient de l'usurpation, que d'autres étaient plus proches de la fraude et que d'autres encore comprenaient des éléments soit des deux, soit ni de l'un ni de l'autre, et seraient mieux qualifiées d'"infractions connexes".

4. Le terme général "criminalité identitaire" s'entend de toutes les formes de comportement illicite ayant trait à l'identité, y compris de l'usurpation d'identité et de la fraude à l'identité. Son usage est nécessairement néologique, la plupart des États n'ayant pas encore adopté de lois relatives à de telles infractions. En général, le terme englobe les infractions tant préparatoires que constitutives, telles que la falsification ou l'usurpation, mais un problème terminologique se pose du fait que l'abus d'identité peut porter sur les informations relatives à l'identité elles-mêmes ou sur d'autres informations s'y rapportant, auquel cas il n'est pas forcément question de "criminalité identitaire", bien que les effets soient généralement les mêmes. Aux fins de la présente étude, on a employé le terme plus général de "criminalité liée à l'identité" de manière à englober de telles situations. Dans certains contextes, on emploie aussi le terme "abus d'identité" dont le sens est proche, mais qui ne présuppose pas qu'un acte constitue une infraction pénale ou devrait être érigé comme tel. La notion de fausse identité ou de falsification d'identité ou de pièces d'identité couvre trois types d'actes abusifs, à savoir: le fait d'inventer ou de forger une identité entièrement fictive; le fait de modifier ou d'utiliser en partie une identité authentique; et le fait pour une personne autre que son titulaire légitime, ou dans le cas d'un document, autre que son détenteur légitime, d'utiliser une identité authentique[3].

---

[3] *Travaux préparatoires des négociations relatives à l'élaboration de la Convention des Nations Unies contre la criminalité transnationale organisée* (publication des Nations Unies, numéro de vente: F.06.V.5), deuxième partie, art. 12, sect. C, note interprétative b), et troisième partie, art. 12, sect. C, note interprétative b).

5. Le terme “usurpation d’identité” désigne généralement le fait de prendre des informations liées à l’identité, qui peuvent être des informations de base, voire d’autres informations personnelles, d’une manière analogue au vol ou à la fraude (y compris le vol de documents tangibles et d’informations intangibles); le fait de prendre des documents ou des informations qui ont été abandonnés ou qui sont librement accessibles; et le fait de convaincre des individus par des moyens frauduleux de remettre volontairement des documents ou des informations. Le terme “fraude à l’identité” quant à lui désigne généralement l’usage d’informations d’identification ou de pièces d’identité pour commettre d’autres infractions ou pour échapper d’une certaine manière à la détection et aux poursuites. L’élément de tromperie porte non sur l’obtention des informations, mais sur l’usage ultérieur qui en est fait pour tromper autrui. Comme pour la fraude économique, l’élément de tromperie vise aussi bien les systèmes techniques que les êtres humains.

II. Le fondement de l’identité: moyens d’identification utilisés par les États Membres

A. Systèmes d’identification publics et privés

6. La plupart des États ont signalé qu’ils disposaient d’infrastructures à la fois publiques et privées pour l’identification et ont décrit divers moyens d’identification destinés à des applications particulières. Pour ce qui est de l’identification dans le secteur public, certains États ont fait état de programmes d’identification nationaux centralisés, mais la plupart semblaient faire fond principalement sur l’identification établie à des fins spécifiques (permis de conduire, passeports, certificats de naissance, certificats de citoyenneté) et sur celle utilisée dans le régime public des impôts et des allocations. Dans le secteur privé, l’identification était généralement émise à des fins commerciales spécifiques, par exemple bancaires ou financières, mais des formes d’identification plus généralisées, créées par des entreprises spécialisées dans ce domaine, semblaient émerger. Certains pays avaient combiné les deux méthodes, et dans certains États ayant un système fédéral, les États ou les provinces avaient leurs propres programmes d’identification, ce qui avait nécessité la mise en place de normes communes de vérification aux échelles tant nationale qu’internationale. Là où aucun système d’identification national n’existait, on avait tendance à utiliser des formes d’identification spécifiques à des fins autres que celle d’origine, à la fois par nécessité et, conformément au principe de redondance, dans un souci de fiabilité supplémentaire. La forme d’identification commerciale privée la plus couramment mentionnée était la carte de crédit. Les avis sur les systèmes d’identification nationaux ont divergé. Dans certains pays, les règles nationales d’identification étaient largement acceptées, mais dans d’autres, les propositions en ce sens avaient suscité des controverses et des objections pour des motifs de protection des libertés civiles. Un État a fait observer que son système national d’identification était de plus en plus fréquemment exploité à des fins commerciales et s’est demandé s’il faudrait demander aux parties commerciales intéressées de participer aux frais élevés encourus pour la gestion d’un système centralisé.

B. La notion d'informations d'identification

7. La notion d'informations d'identification était nouvelle pour la plupart des États. Peu l'avaient reconnue en termes juridiques ou législatifs, même si les États qui examinaient la question de la criminalité liée à l'identité avaient commencé à l'envisager. La plupart des États ont plutôt mentionné les documents d'identification ou les informations personnelles, lesquelles englobaient les informations d'identification ainsi que d'autres informations personnelles ou confidentielles sur le statut ou les activités des personnes identifiées, qui n'étaient pas nécessairement suffisantes pour identifier un individu. De nombreux États ont indiqué avoir formulé des lois pénales et d'autres mesures pour protéger les informations personnelles, y compris la plupart ou la totalité des informations d'identification. Beaucoup ont aussi fait état d'infractions, telles que le vol, la fraude, le trafic ainsi que la possession ou l'usage illicites, qui portaient spécifiquement sur certaines pièces comme les passeports. Il importe de noter concernant cette notion que les éléments constitutifs des informations d'identification sont nécessaires mais, pris isolément, ne suffisent généralement pas pour établir l'identité. Les pièces d'identité les plus courantes comportent en fait plusieurs de ces éléments, et les moyens d'identification automatisés comme les cartes de débit et de crédit en requièrent généralement au moins deux: l'un provenant de la carte ou du document et l'autre de l'individu identifié. Les approches de la question de savoir ce qui constitue des informations d'identité peuvent varier dans une certaine mesure en fonction de facteurs culturels et de traditions locales. Dans certaines culture, le nom des parents, l'origine familiale, ou la profession sont incorporés dans le nom. Un autre facteur concerne la mesure dans laquelle la reconnaissance traditionnelle du face-à-face a été remplacée dans un premier temps par des documents papier et, plus récemment, par l'identification électronique, à mesure que de nouvelles formes d'informations d'identification ont été créées.

8. Les informations le plus souvent mentionnées pour les documents papier étaient les suivantes: les noms divers (prénom, nom usuel, nom des parents), le lieu et la date de naissance et le lieu actuel de résidence ou d'exercice; et pour les systèmes électroniques: le nom complet ou le nom d'utilisateur abrégé, les mots de passe, les codes secrets, les numéros de transaction (TAN), les signatures numériques et d'autres applications cryptographiques. Un nouveau domaine de développement concernant l'appui technologique est celui des divers identifiants biométriques, à savoir notamment les données ADN, les empreintes digitales, les photographies, les empreintes vocales, ainsi que les images de l'iris ou de la rétine. Les photographies, faciles à utiliser, sont courantes, mais les autres identifiants biométriques, s'ils présentent un haut degré de sécurité, sont coûteux et soulèvent des questions de confidentialité; ils ne sont donc répandus que dans des domaines comme celui des casiers judiciaires, où les coûts se justifient par un besoin de sécurité ou d'autres facteurs. Deux États ont indiqué prévoir des dispositions, notamment législatives, sur la question. L'un a employé le terme "identification data" (données d'identification) pour désigner des informations électroniques constitutives d'identification dans un système automatisé. Un autre a indiqué prévoir la définition législative suivante du terme "means of identification" (moyen d'identification) dans le contexte d'infractions liées à l'usurpation d'identité: "tout nom ou numéro qui, seul ou combiné avec d'autres informations, peut être utilisé pour identifier un individu particulier".

III. Criminalité liée à l'identité

A. Types d'infractions

9. Les États ont fait état de diverses infractions impliquant l'usage impropre ou la falsification de l'identité à des fins criminelles. Les infractions courantes comprenaient la falsification de pièces d'identité et divers types d'usurpation d'identité. Outre les infractions portant sur des documents d'identification, on a signalé celles qui ciblaient les systèmes ou les processus utilisés pour créer, établir ou vérifier l'identité. Une façon de manipuler ces systèmes consistait à essayer d'induire en erreur ou d'altérer le processus de délivrance afin d'attribuer une identification valable à une personne qui n'y avait pas droit. Plusieurs États ont signalé des infractions de cette nature, à la fois de corruption générale et d'autres actes plus spécifiques liés à l'utilisation d'informations fausses ou trompeuses afin d'obtenir des permis ou d'autres pièces d'identité. Certains moyens d'obtenir illicitement des informations relatives à l'identité étaient visés par les lois en vigueur sur le vol, mais ces dernières risquaient de ne pas toujours s'appliquer. En effet, les informations intangibles n'étant pas toujours considérées comme des biens, les lois sur le vol pouvaient ne pas s'appliquer lorsque ces informations étaient tirées de documents mis au rebut par exemple. Les lois en vigueur sur la fraude économique pouvaient s'appliquer à des pratiques comme le "phishing" ou "hameçonnage" s'il était possible d'établir que les informations acquises frauduleusement présentaient un grand intérêt. Quelques États ont indiqué prévoir des lois sur d'autres infractions, notamment sur la possession, le transfert ou le trafic illicites d'identités ou d'informations telles que des mots de passe informatiques et des données de cartes de crédit. Plusieurs États s'inquiétaient de la possibilité pour les auteurs d'infractions d'obtenir de grandes quantités d'informations par piratage informatique. Un certain nombre d'États ont mentionné diverses formes d'usurpation d'identité, notamment le fait de s'approprier l'identité d'une autre personne ou de créer de toutes pièces l'identité d'une personne fictive et de se l'approprier.

B. Moyens utilisés pour commettre des infractions liées à l'identité

10. Les réponses au questionnaire ont montré que les techniques de la criminalité liée à l'identité dépendaient dans une certaine mesure de la nature et de l'objet des structures d'identification visées et des moyens dont disposaient les délinquants. Dans la plupart des cas, des informations d'identification étaient prises, copiées ou falsifiées de façon plausible, converties en une forme utilisable et exploitées. Les délinquants obtenaient les informations en volant ou en copiant des documents entiers ou en acquérant, par divers moyens, des informations partielles, dans le but de créer des identités et d'obtenir des documents authentiques. Certains États ont signalé des cas où l'identité d'une personne décédée jeune était récupérée et servait à faire de fausses demandes de certificats de naissance et d'autres informations d'identification de base pour progressivement construire une identité complète. Un nombre important d'États s'est dit préoccupé par la criminalité liée à l'identité qui faisait des victimes chez les utilisateurs des technologies de l'information. La méthode la plus fréquemment utilisée était le "hameçonnage" ou le "pharming", grâce à laquelle les délinquants amenaient frauduleusement des utilisateurs de

réseaux informatiques à leur communiquer noms d'utilisateurs, mots de passe et autres informations d'identification électroniques. Ils s'adressaient aux victimes par courrier électronique ou sur des sites Web pour leur demander ces informations en se faisant passer pour des fournisseurs de services ou d'autres organismes. Les sites en question étaient souvent hébergés dans des pays éloignés à la fois des délinquants et des victimes, et un État a indiqué en avoir retrouvé la trace dans au moins 10 pays différents. D'autres formes de cybercriminalité avaient aussi été rencontrées, notamment la contamination d'ordinateurs personnels par des logiciels malveillants qui interceptaient des informations personnelles pour les transmettre aux délinquants, et le piratage de sites Web commerciaux pour obtenir les données de cartes de crédit et d'autres informations d'identification des clients. Les informations d'identification, surtout en grandes quantités, étaient devenues une marchandise illicite vendue entre délinquants. Des entités commerciales soucieuses de la confiance de leur clientèle avaient été victimes d'un chantage perpétré par des délinquants qui s'emparaient d'informations et menaçaient de les publier à défaut d'être payés.

11. Un certain nombre d'États ont signalé des méthodes utilisées pour obtenir les informations d'identification de cartes de débit et de crédit, avant tout à des fins de fraude économique. Certaines informations étaient recueillies grâce à une technique appelée "skimming" (où la carte était passée dans un lecteur de données). Dans le cas des cartes de débit, ces lecteurs étaient fixés au distributeur automatique et assortis d'une caméra miniature qui enregistrait le code secret de l'utilisateur. D'autres États ont signalé des cas où des informations d'identification étaient obtenues par des fonctionnaires ayant un accès privilégié aux systèmes publics ou commerciaux ou par des délinquants de l'extérieur au moyen d'actes de corruption et d'autres techniques frauduleuses. Les informations ainsi obtenues pouvaient fréquemment être exploitées sur-le-champ pour usurper l'identité de la victime tandis que pour les pièces d'identité matérielles, d'autres opérations étaient souvent nécessaires. Du fait que les documents d'identification matériels étaient devenus plus complexes, leur falsification exigeait davantage de savoir-faire, de ressources et de matériel, ce qui supposait l'implication ou l'appui de groupes criminels organisés. Cependant, les technologies de l'information et de la communication avaient permis à un grand nombre de délinquants agissant seuls d'accéder à certains moyens de falsification, ce qui avait fait évoluer à la fois les techniques de protection des documents et les techniques criminelles. Outre la falsification de documents matériels, des infractions liées à l'identité avaient aussi été commises par altération des systèmes auxquels les documents étaient rattachés.

C. Mesures juridiques

12. Un assez large consensus semblait se dégager sur le fait que certaines formes d'abus d'identité devaient être érigées en infraction pénale et passibles de sanction, mais les avis étaient quelque peu divergents sur le point de savoir quels types d'actes précisément il convenait d'incriminer. La plupart des États avaient classé les infractions liées à l'identité dans des catégories plus générales. Cependant, seuls six États ont indiqué avoir incriminé, totalement ou partiellement, le transfert, la possession ou l'utilisation de l'identité ou des informations d'identification d'autrui ou encore d'une fausse identité dans le cadre d'une autre infraction, dont un

seulement (les États-Unis d'Amérique) avait incriminé l'usurpation d'identité en tant que telle. La loi pertinente des États-Unis définissait les "moyens d'identification" et incriminait la possession, le transfert et l'utilisation sans autorisation et en connaissance de cause de ces informations. Plusieurs autres États ont indiqué étudier les concepts qui sous-tendaient les infractions fondées spécifiquement sur l'abus d'identité, notamment le fait de prendre, de créer de toutes pièces et d'utiliser abusivement des informations d'identification y compris dans le but de commettre d'autres infractions pénales. Presque tous les États ont signalé qu'ils avaient incriminé au moins certains des faits évoqués dans la description de la fraude à l'identité proposée dans le questionnaire, ou des faits connexes. Les infractions les plus fréquemment décrites étaient celles qui se rapportaient à la falsification et à l'usurpation. Certains abus d'identité étaient aussi considérés comme des éléments d'infractions plus générales. Par exemple, la falsification englobait la falsification de pièces d'identité et la cybercriminalité le vol de données, l'accès sans droit à des systèmes informatiques et leur altération. Quelques États ont indiqué avoir incriminé les infractions liées à certains types d'identification ou d'identité jugés particulièrement importants, comme les passeports ou les documents délivrés par les pouvoirs publics. Les États parties à la Convention sur la cybercriminalité étaient tenus, en vertu de l'article 7, de faire en sorte que leurs lois sur la falsification couvrent la falsification informatique ou la falsification de données informatiques. Plusieurs États ont signalé des infractions liées au "hameçonnage" ou à des actes connexes. Dans d'autres États, cette pratique pouvait aussi être visée par les lois plus générales sur la cybercriminalité, par exemple sur le vol ou la possession illicite de mots de passe.

IV. Relation entre la criminalité liée à l'identité et d'autres éléments

A. Relation entre la criminalité liée à l'identité et la fraude économique

13. Si la présente étude fait une distinction entre la fraude économique et les infractions liées à l'identité, les données disponibles tendent à montrer qu'il y a dans la pratique d'importants chevauchements. Tel est aussi l'avis de certains États dont les experts en matière de fraude économique ont assumé le gros du travail dans le nouveau domaine de la criminalité identitaire. C'est une raison pour laquelle la Commission pour la prévention du crime et la justice pénale a décidé de mener cette étude sur une base commune. Comme il a été noté, l'abus d'identité joue à peu près le même rôle pour la fraude économique que pour d'autres infractions, en plus de l'élément de tromperie des victimes présent dans de nombreuses manœuvres frauduleuses. Maints exemples en ont été donnés. Des auteurs de fraude économique se faisaient passer pour des fonctionnaires afin d'obtenir des informations ou de récupérer le produit d'une fraude antérieure en présentant des réclamations non fondées. L'usurpation de l'identité d'agents bancaires, d'émetteurs de carte de crédit et de fournisseurs de télécommunications était une forme courante de fraude économique ou de fraude aux télécommunications. L'utilisation de fausses identités était aussi un élément important dans de nombreux cas d'usurpation, notamment dans le cadre du "hameçonnage" où les délinquants se faisaient passer pour tel ou

tel organisme afin d'amener les victimes à leur communiquer des mots de passe informatiques ou d'autres informations d'identification. Certains États ont signalé des actes qui pourraient servir de base à des infractions, par exemple lorsque l'usurpation d'identité et la fraude à l'identité servaient à des manœuvres frauduleuses plus importantes. Certains actes frauduleux comme la fraude à la carte bancaire pouvaient aussi être qualifiés de fraude à l'identité car l'auteur de l'infraction s'identifiait avec une carte copiée ou volée et usurpait de fait l'identité du titulaire légitime. Dans les systèmes commerciaux comme celui des cartes de crédit, le fondement de l'identité était souvent si étroitement lié aux aspects commerciaux qu'il était difficile, voire impossible, de distinguer la fraude à l'identité de la fraude économique.

14. Une différence essentielle entre la fraude et la criminalité liée à l'identité était que, pour la quasi-totalité des États ayant répondu au questionnaire, la première était considérée comme une infraction économique dans les définitions juridiques et les lois. D'où la nécessité d'apporter la preuve d'une certaine perte matérielle pour la victime ou d'un certain gain matériel pour le délinquant. En réalité, les infractions liées à l'identité n'étaient pas nécessairement de nature économique et pouvaient être commises pour faciliter d'autres infractions, économiques ou non. Cette différence pouvait par ailleurs avoir une incidence sur l'application de la Convention contre la criminalité organisée. En effet, cette dernière ne s'applique qu'en présence d'un groupe criminel organisé lequel, conformément à la définition qu'elle prévoit, a notamment pour objectif de dégager "un avantage financier ou un autre avantage matériel"[4]. De ce fait, un groupe organisé, par exemple terroriste, dont les objectifs n'auraient aucun caractère économique, et toutes infractions liées à l'identité qu'il commettrait, n'entreraient pas dans le champ d'application de la Convention. En revanche, la grande majorité des autres cas seraient visés. Premièrement, la Convention précise que ce sont les objectifs du groupe, et non les infractions particulières qu'il pourrait commettre, qui doivent impliquer un avantage financier ou un autre avantage matériel. Cela signifie que des infractions non économiques liées à l'identité seraient visées par la Convention si elles pouvaient être attribuées à un groupe criminel organisé qui commet aussi des infractions économiques. La Convention s'appliquerait à des cas où des infractions liées à l'identité servent à faciliter la traite de personnes, le trafic de migrants, le blanchiment d'argent ou d'autres formes de traite ou de trafic, même si la phase initiale des enquêtes ne met en évidence aucun lien manifeste outre l'appartenance au groupe lui-même. Deuxièmement, la formule "un avantage financier ou un autre avantage matériel" a un sens relativement large, incluant par exemple le trafic de matériels pornographiques impliquant des enfants pour des motifs de gratification sexuelle (A/55/383/Add.1, par. 3)[5]. Elle englobe les infractions liées à l'identité où des informations d'identification ou des pièces d'identité volées ou créées de toutes pièces sont traitées comme une forme de marchandise illicite, en d'autres termes achetées, vendues ou échangées, ainsi que les cas d'usage impropre de l'identité dans le but de dégager des avantages personnels ou collectifs, y compris non financiers, par exemple pour s'assurer l'entrée dans un autre pays. Troisièmement,

[4] Voir la Convention contre la criminalité organisée, alinéa a) de l'article 2, et le paragraphe 1 de l'article 3.

[5] *Travaux Préparatoires...*, première partie, art. 2, sect. C, note interprétative d). Voir aussi A/AC.254/4/Rev.1, note 4; A/AC.254/4/Rev.2, note 16; et A/AC.254/4/Rev.7, note 22.

d'après les rapports reçus, il semble que les infractions les plus couramment associées à la criminalité liée à l'identité soient de nature économique, telles que les fraudes et les infractions portant sur les documents de voyage et les pièces d'identité, qui entrent dans le champ d'application du Protocole visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants et du Protocole contre le trafic illicite de migrants par terre, air et mer, additionnels à la Convention des Nations Unies contre la criminalité transnationale organisée (résolution 55/25 de l'Assemblée générale, annexes II et III). On avait présumé que ces infractions impliquaient un avantage financier ou un autre avantage matériel, sauf dans les cas de trafic de migrants à des fins humanitaires ou à d'autres fins non criminelles[6].

B. Autres infractions associées à la criminalité liée à l'identité

15. Les liens signalés entre la criminalité liée à l'identité et d'autres infractions pouvaient être répartis en trois catégories selon l'usage fait des identités fausses ou usurpées: premièrement, pour accéder à des lieux physiques ou des comptes électroniques afin de commettre d'autres infractions; deuxièmement, pour dissimuler l'identité réelle du délinquant et échapper à la détection, aux entraves et aux poursuites; et troisièmement, dans le cas de la fraude économique, comme élément de l'infraction principale dans une manœuvre frauduleuse.

16. Si les liens entre l'abus d'identité et d'autres infractions portaient le plus souvent sur l'identité des délinquants, l'identité des victimes pouvait aussi entrer en jeu. De nombreux rapports de pays sur la traite des personnes signalaient que les auteurs d'infractions confisquaient les passeports ou les pièces d'identité de leurs victimes afin de les contrôler ou de les empêcher de fuir. Bien que le Protocole relatif à la traite des personnes ne l'exige pas, certains États parties avaient incriminé la privation de l'identité dans ce contexte[7]. Le paragraphe 1 de l'article 7 de la Convention des Nations Unies relative aux droits de l'enfant (résolution 44/25 de l'Assemblée générale, annexe) établit le droit de l'enregistrement à la naissance comme moyen de déterminer l'identité; la privation systématique d'identité a été observée dans des cas de génocide et de nettoyage ethnique[8].

17. Les infractions relatives à l'identité sont le plus fréquemment liées à la fraude économique et aux infractions connexes, en partie du fait que la fraude économique est très courante dans la plupart des États et que l'abus d'identité joue un rôle très important dans la réussite de la plupart des actes de fraude. Un certain nombre d'États a signalé que la criminalité identitaire servait dans des cas de blanchiment d'argent à déjouer les mécanismes de détection du produit du crime et des

---

[6] La définition du "trafic de migrants" doit faire référence à "un avantage financier ou un autre avantage matériel" pour que les États parties ne soient pas tenus d'incriminer le trafic à des fins non criminelles, par exemple humanitaires, ou le trafic de proches (Voir le Protocole relatif aux migrants, alinéa a) de l'article 2, ainsi que les *Travaux préparatoires...*, troisième partie, art. 3, sect. C, note interprétative a)).

[7] Voir, par exemple, le *Code criminel du Canada*, art. 279.03 sur la rétention ou la destruction de documents de voyage ou d'identité (Lois du Canada (2005), chap. 43).

[8] Voir, par exemple, *Procureur du Tribunal pénal international pour l'ex-Yougoslavie contre Slobodan Milosevic et al*, affaire n° IT-99-37-PT, deuxième acte d'accusation modifié (29 octobre 2001), par. 61 (http://www.un.org/icty/indictment/french/milu-2ai011029f.htm).

opérations suspectes. De nombreux États se sont dits particulièrement préoccupés par les infractions liées à l'identité qui portaient sur des passeports et d'autres documents de voyage, considérant qu'il s'agissait à la fois d'un problème de criminalité et d'un problème de sécurité, les passeports étant essentiels pour empêcher l'entrée sur leur territoire de terroristes connus, d'auteurs d'infractions pénales et de migrants clandestins. L'usage illicite de passeports était aussi rattaché à la criminalité organisée, notamment par la traite des personnes ou le trafic de migrants, et un certain nombre d'États qui ont signalé ces liens ont fait état de taux élevés de trafic et de traite en raison de leur situation géographique. Plusieurs États ont indiqué avoir créé de nouveaux passeports présentant des mesures de sécurité supplémentaires. Par ailleurs, un certain nombre de liens entre la criminalité liée à l'identité et la cybercriminalité avaient été observés. Plusieurs États ont signalé, outre des manœuvres frauduleuses en vue d'obtenir des informations d'identification informatiques, l'usage de fausses identités et de fausses cartes de crédit pour bénéficier de services de télécommunications intraçables et se livrer à d'autres infractions, notamment des actes terroristes.

C. Relation entre la criminalité liée à l'identité et la criminalité organisée

18. Un certain nombre d'États ont signalé des liens entre la criminalité liée à l'identité et des groupes criminels organisés. Les cas les plus fréquents concernaient la fraude économique organisée, le blanchiment d'argent, la traite des personnes, le trafic de migrants ou la fraude destinée à bénéficier de télécommunications intraçables. Ces questions sont abordées ailleurs dans le présent rapport. Outre les infractions liées à l'identité commises dans le cadre d'activités criminelles telles que le blanchiment d'argent, certains groupes criminels pourraient disposer de moyens suffisamment complexes pour commettre ces infractions en tant qu'activité criminelle distincte. Les réponses des États ont mis en évidence deux cas de figure principaux: les groupes criminels organisés pouvaient avoir recours à la criminalité liée à l'identité pour protéger leurs membres et leurs agissements contre les mécanismes de surveillance des activités illicites, ou pour mener leurs activités courantes non délictueuses comme les voyages internationaux. Selon d'autres informations, certains groupes se spécialisaient dans ce domaine et traitaient les pièces d'identité et les informations d'identification comme une marchandise illicite. Ces groupes pourraient acquérir les compétences spécialisées nécessaires pour créer de fausses pièces d'identité de plus en plus élaborées ou pour exploiter les lacunes des systèmes de délivrance, en trompant ou en corrompant les autorités concernées afin d'obtenir des document authentiques pouvant ensuite être vendus à d'autres et servir à la commission d'infractions et d'actes de terrorisme, à des déplacements illicites, à des migrations et à d'autres activités où l'identité légitime serait compromettante. Certains groupes criminels organisés étaient suffisamment ingénieux pour se livrer à des manœuvres identitaires complexes, où les informations d'identité provenant d'une certaine source étaient utilisées pour présenter de fausses demandes de documents authentiques, l'objet étant d'élaborer et de conserver des identités fictives encore plus solides et plus complexes.

D. Relation entre la criminalité liée à l'identité et le terrorisme

19. Seuls quelques États ont soulevé la question des liens entre la criminalité liée à l'identité et le terrorisme. Leur préoccupation principale à cet égard était essentiellement la même que celle suscitée par la criminalité organisée et d'autres problèmes, à savoir que les organisations terroristes pourraient recourir à la criminalité liée à l'identité pour obtenir des informations et des documents d'identification qui, à leur tour, pourraient leur permettre d'échapper à la surveillance ou à une arrestation (situation probable si leur identité authentique était connue). Dans ce contexte, les États se focalisaient sur les voyages et les déplacements internationaux de suspects terroristes[9], mais les mêmes problèmes se posaient concernant l'identification et les activités au niveau purement interne, étant donné que les terroristes devaient aussi éviter de se faire remarquer au quotidien, par exemple au volant d'une voiture ou lors d'opérations bancaires, et que les formes courantes d'identification interne servaient de base pour obtenir des pièces plus sécurisées comme des passeports, l'identification relative à l'emploi et les documents connexes, qui étaient nécessaires pour se rendre dans des lieux sécurisés comme les aéroports.

20. D'autres sources officielles consultées par des experts donnaient des exemples de suspects terroristes qui obtenaient et utilisaient des pièces d'identité pour échapper à la surveillance et aux contrôles. Il s'agissait notamment de documents falsifiés ou modifiés et de documents authentiques obtenus avec de faux noms, dont les informations essentielles, telles que le nom et la date de naissance, n'identifiaient pas correctement l'utilisateur et n'étaient pas rattachées à des antécédents compromettants. Une autre manœuvre consistait à déposer des demandes frauduleuses ou trompeuses pour obtenir de nouveaux documents. Des complices pouvaient simplement remettre les documents à des organisations terroristes et prétendre ensuite qu'ils avaient été perdus ou volés. En outre, les suspects dont les passeports indiquaient des déplacements compromettants pouvaient les détruire et obtenir frauduleusement leur remplacement[10]. Une autre préoccupation soulevée dans ce contexte par certains États concernait, comme pour la fraude économique, les cas de fraude générale contre des fournisseurs de télécommunications dans le but d'obtenir de façon anonyme et intraçable des services de téléphonie mobile et d'Internet et d'autres services de télécommunications.

21. En l'absence de données précises, il peut être difficile de distinguer la criminalité liée à l'identité et associée au terrorisme des infractions connexes, notamment de la criminalité organisée. De nombreux modes opératoires de base sont communs aux groupes à la fois criminels et terroristes et les seconds, lorsqu'ils n'ont pas eux-mêmes les compétences spécialisées nécessaires, peuvent simplement acheter de faux documents d'identification aux premiers. Les infractions liées à l'identité peuvent servir au financement du terrorisme, essentiellement de la même manière qu'au blanchiment d'argent.

---

[9] Voir, par exemple, le rapport du Secrétaire général intitulé: "S'unir contre le terrorisme: recommandations pour une stratégie antiterroriste mondiale" (A/60/825, par. 62).

[10] Voir par exemple le *Rapport de la Commission nationale sur les attentats terroristes contre les États-Unis d'Amérique* (*Report of the National Commission on Terrorist Attacks upon the United States*, chapitre 5.3, p. 168 et 169 (http://www.9-11commission.gov/report/index.htm).

E. Relation entre la criminalité liée à l'identité et le blanchiment d'argent

22. De nombreuses mesures de lutte contre le blanchiment d'argent reposent en grande partie sur l'identité ou sur des éléments d'identification, et les moyens utilisés par les délinquants pour blanchir le produit de leurs infractions font intervenir la criminalité liée à l'identité. La capacité d'identifier les clients et les parties à des transactions financières, aussi appelée le principe "connaissez votre client", de même que la conservation de documents financiers et l'obligation de signaler les activités suspectes, constitue un élément fondamental des programmes de lutte contre le blanchiment d'argent[11]. L'identification des parties à une transaction peut aider à déterminer l'origine illicite de fonds ou d'avoirs et contribuer aux enquêtes sur les infractions accessoires et principales. À un stade ultérieur, il est généralement essentiel d'identifier toutes les parties impliquées dans une suite de transferts à des fins de blanchiment, de manière à poursuivre les auteurs, à tracer le produit et les fonds ou avoirs dérivés et à établir de façon suffisamment certaine les liens de causalité ou de continuité entre les infractions principales et la forme et le lieu finals du produit pour justifier une confiscation pénale. S'agissant des infractions principales, les processus d'identification fiables remplissent aussi une certaine fonction de contrôle et de dissuasion[12]. Certains États ont fait observer que les techniques de blanchiment d'argent exploitaient les technologies de l'information, de la communication et du commerce, lesquelles permettaient de générer de fausses informations d'identification, d'effectuer des transferts à distance à l'aide de ces fausses identités et de faire d'importants transferts légitimes parmi lesquels les avoirs d'origine illicite pouvaient être dissimulés. Ces technologies avaient par ailleurs entraîné une expansion considérable des transferts internationaux et des activités bancaires extraterritoriales, ce qui avait créé des obstacles à la réglementation et rendu les banques extraterritoriales et les techniques de dissimulation accessibles à un éventail de délinquants beaucoup plus large. Cela dit, les nouvelles technologies avaient également permis des développements parallèles dans le domaine de l'appui à la prévention du crime, à la sécurité et aux enquêtes.

F. Relation entre la criminalité liée à l'identité et la corruption

23. Il n'était pas demandé aux États Membres d'aborder le rapport entre la criminalité liée à l'identité et la corruption, mais les experts ont examiné certains liens possibles. Comme pour les autres infractions, la criminalité liée à l'identité pourrait offrir un moyen d'échapper à la détection ou à la responsabilité pénale lorsque des actes de corruption sont commis. Par exemple, de fausses identités pourraient servir à déjouer les enquêtes sur des infractions telles que le

---

[11] Voir par exemple le paragraphe 1 a) de l'article 7 de la *Convention contre la criminalité organisée*, l'article 14 de la *Convention des Nations Unies contre la corruption*; et la Recommandation 5 des quarante Recommandations du Groupe d'action financière sur le blanchiment de capitaux (GAFI) (http://www.fatf-gafi.org/document/23/0,2340, fr_32250379_32236920_34920215_1_1_1_1,00.html#rec5).

[12] Voir P. A. Schott, *Guide de référence sur la lutte contre le blanchiment de capitaux et le financement du terrorisme* (Banque mondiale, 2003), chap. VI, partie A.

détournement de fonds. Comme pour le blanchiment d'argent, l'abus d'identité pourrait aussi servir à empêcher la localisation et la confiscation du produit d'actes de corruption. L'autre facette essentielle de cette relation était le recours à la corruption pour faciliter les infractions liées à l'identité. Par exemple, du fait qu'il est aujourd'hui plus difficile de falsifier les passeports ou des pièces analogues ou d'en créer de faux, une solution plus simple dans de nombreux cas consiste à corrompre activement ou passivement des fonctionnaires pour obtenir un document authentique. De même, on pourrait recourir à la corruption pour modifier ou falsifier des informations dans des systèmes utilisés pour valider ou vérifier l'identité. Ce domaine étant considéré nouveau, les experts étaient d'avis que de telles situations risquaient de se présenter à mesure de l'expérience acquise.

G. Relation entre la criminalité liée à l'identité et les technologies de l'information, de la communication et du commerce

24. Comme pour la fraude économique, les technologies de l'information et de la communication jouent un rôle complexe dans la criminalité liée à l'identité. Dans certains cas examinés, elles formaient un élément essentiel de l'infraction tandis que dans d'autres, elles n'étaient qu'un élément accessoire. En matière d'identification, la dépendance accrue aux technologies, par opposition au contact humain, avait créé de nouvelles possibilités d'usurpation, le fait de connaître des mots de passe et d'autres identifiants étant suffisant pour corrompre des systèmes automatisés, quelle que soit l'identité réelle de l'auteur. L'expansion des technologies avait aussi permis à un grand nombre de délinquants relativement peu expérimentés d'accéder à des moyens élaborés pour falsifier des documents tant matériels qu'électroniques. En outre, grâce aux nouvelles technologies, il était possible de corrompre les systèmes de délivrance pour obtenir des documents authentiques. Cela dit, l'évolution technologique comportait aussi des éléments tendant à prévenir ou à réprimer la criminalité liée à l'identité, dont certains étaient inhérents aux nouvelles technologies, d'autres y avaient été intégrés spécifiquement pour prévenir la criminalité ou faciliter la détection et les enquêtes, et d'autres encore avaient été élaborés et commercialisés aux fins spécifiques de combattre les nouvelles formes de criminalité qui avaient émergé. Les mesures de précaution comprenaient l'incorporation dans les documents, pour rendre leur production plus difficile, d'éléments physiques tels que des photographies, des caractères microscopiques, des hologrammes et des puces informatiques qui nécessitaient encore du matériel et des connaissances relativement complexes. En outre, grâce aux télécommunications modernes sécurisées, il était possible de rapidement vérifier l'authenticité des pièces d'identité dans des bases de données sécurisées multiples; et grâce aux technologies de l'information, ce processus était suffisamment rapide pour servir à des applications telles que le contrôle aux frontières. Un État a noté que là où c'était possible, on recourait de plus en plus à l'identification dite multifactorielle, où divers identifiants étaient enregistrés séparément et vérifiés par recoupement dès qu'il fallait établir ou contrôler l'identité. Les éléments visés étaient de trois types principaux: les éléments matériels en la possession du sujet, tels qu'une carte bancaire, une carte d'identité nationale, un passeport; les éléments que seuls le sujet connaissait, tels qu'un mot de passe ou un code confidentiel; et les éléments biologiquement uniques du sujet (les éléments biométriques).

H. Éléments transnationaux et nécessité d'une coopération internationale contre la criminalité liée à l'identité

25. Un certain nombre d'États ont signalé avoir observé des cas d'infractions liées à l'identité présentant des aspects transnationaux. La majorité concernait des passeports ou d'autres documents de voyage. Les infractions étaient soit liées directement aux documents d'identification (faux papiers, falsification, usage abusif de documents authentiques ou de processus de délivrance), soit commises en partie par l'usage impropre de ces formes d'identification (traite de personnes, trafic de migrants et autres infractions liées à l'entrée et à l'immigration illégales). Les informations d'identification numériques étaient faciles à transmettre au niveau international. L'autre grande catégorie d'infractions liées à l'identité dont il a souvent été dit qu'elle présentait des aspects transnationaux était la cybercriminalité.

26. Plusieurs États ont souligné l'importance de la coopération internationale pour les enquêtes et les poursuites dans le domaine de la criminalité transnationale liée à l'identité, mais ils n'ont pas précisé les formes particulières de coopération nécessaires. Comme pour la fraude économique, la plupart des États ont considéré que les cadres existants, tels que la Convention contre la criminalité organisée, la Convention des Nations Unies contre la corruption et la Convention sur la cybercriminalité, étaient suffisants. Plusieurs ont aussi mis l'accent sur l'utilité, en termes pratiques, d'Interpol, de l'Office européen de police (Europol) et d'organismes analogues en tant que mécanismes de coopération. La plupart des États ont estimé que les formes de coopération spécifiques qui étaient nécessaires dans ce domaine étaient à peu près les mêmes que pour la fraude transnationale et d'autres formes de cybercriminalité. La plupart des infractions majeures commises avec une fausse identité ou une identité volée étaient susceptibles d'être considérées comme des "infractions graves" au sens de l'alinéa b) de l'article 2 de la Convention contre la criminalité organisée, mais les États commençant à traiter les abus d'identité comme une infraction distincte, la question se poserait de savoir si les nouvelles infractions spécialisées entraient aussi dans le champ d'application de cette convention. Plusieurs États ont noté que, comme pour la cybercriminalité, la rapidité tant de l'assistance officielle que de la coopération informelle jouait parfois un rôle capital. À cet égard, le réseau 24/7 pouvait être utile dans les cas de fraude où l'on disposait de preuves électroniques, notamment pour les affaires urgentes. Une question que la plupart des États n'ont pas abordée était le fait que, outre les préjudices économiques, les dommages causés par la criminalité liée à l'identité s'étendaient aux personnes physiques et morales touchées. Les atteintes à la réputation et à la viabilité d'une identité de base à des fins personnelles et commerciales, pouvaient être importantes, mais la réparation dans ce contexte n'entrait pas dans les cadres de coopération pénale de la plupart des États.

V. Taux et tendances de la criminalité liée à l'identité

27. Selon l'avis de la plupart des États ayant fourni des données ou des évaluations, la criminalité liée à l'identité connaissait une hausse, qui, pour plusieurs d'entre eux, semblait très rapide. Cette hausse ne concernait pas uniquement le taux global et le nombre de cas, mais aussi le champ et la diversité

des infractions. Seuls deux États ont indiqué une baisse et plusieurs ont signalé que leurs informations étaient insuffisantes ou ne permettaient pas de tirer des conclusions. La plupart ne pouvaient fournir que des avis ou des évaluations d'experts et seul un État a communiqué des statistiques préliminaires, selon lesquelles l'usurpation d'identité était un problème important et croissant. Le concept était si nouveau que toute hausse spectaculaire pouvait être attribuée en partie à la meilleure sensibilisation du public au problème, à un accroissement de l'intérêt des pouvoirs publics et à la création récente de services pour la communication de données. Il n'en reste pas moins que les informations ont clairement fait ressortir un nombre important de cas. On a aussi fait état de préjudices économiques majeurs, même s'il n'apparaissait pas clairement dans quelle mesure les pertes résultaient soit de fraudes économiques ou d'infractions accessoires commises par usurpation d'identité, soit d'autres causes comme l'atteinte à la réputation de la victime et le coût du recouvrement de l'identité. Un État a mentionné des études qui montraient que le nombre de sites Web servant au "hameçonnage" avait triplé entre 2005 et 2006. En supposant qu'elles soient exactes, ces données pourraient refléter une tendance selon laquelle les nouvelles formes de criminalité augmentent considérablement sur une courte période lorsque les connaissances techniques s'étendent, puis se stabilisent grâce à une meilleure sensibilisation du public et à des mesures de lutte. Certains États ayant signalé une hausse de la criminalité liée à l'identité ont cité plusieurs causes possibles, comme la corruption de fonctionnaires et des milieux d'affaires, les occasions créées par l'utilisation accrue des technologies informatiques, les obstacles à la création et à l'exécution de mesures techniques de vérification et, en général, la difficulté de suivre le rythme de l'évolution des techniques criminelles. L'absence de définitions claires de la fraude à l'identité et des infractions connexes au niveau national empêche de réaliser des analyses statistiques ou d'aller au-delà des comparaisons très générales entre pays ou régions.

VI. Coût de la criminalité liée à l'identité

28. Aucun des États ayant répondu n'a fourni de données détaillées sur le coût effectif de la criminalité liée à l'identité et seuls quelques-uns avaient estimé les pertes totales. Un certain nombre d'États ont signalé qu'en l'absence de lois spécifiques sur une infraction particulière, on ne pouvait s'attacher à recueillir ou à analyser de façon précise des données statistiques. Par ailleurs, certains États ont noté qu'eu égard à la nature de l'usurpation d'identité, il serait difficile de faire la distinction entre les coûts et les pertes attribuables à cette forme particulière de criminalité et ceux attribuables à d'autres infractions, telles que la fraude, commises avec une identité fausse ou usurpée. Les États qui ont fourni une estimation des pertes totales ont fusionné les chiffres de toutes les infractions principales ayant un lien avec des infractions identitaires, approche que certaines sources commerciales ont également adoptée. Il ressortait de certains exemples qu'il apparaissait difficile de quantifier en termes monétaires quelques-uns des préjudices et des dommages causés, comme les atteintes à la réputation, ou, compte tenu de la durée du préjudice, de fixer une période adaptée pour ce calcul.

29. Selon un État toutefois, il était possible de mener une évaluation qualitative dans laquelle les préjudices et les dommages comprendraient les éléments suivants: les pertes économiques et non économiques susceptibles d'être subies par les personnes dont l'identité était usurpée ou détournée; les coûts, le temps et les efforts mis en jeu pour réparer les dommages causés à l'identité et à la réputation; les pertes économiques et non économiques résultant d'infractions commises en utilisant une identité frauduleuse; les coûts publics et commerciaux de la prévention, des enquêtes et des poursuites; une érosion générale de l'efficacité en raison des mesures de sécurité; et les coûts associés à la perte ou à l'absence de confiance des clients à l'égard des transactions commerciales. Outre la question de la quantification élémentaire, on a aussi soulevé des questions de politique générale sur le point de savoir comment ces coûts devraient être partagés entre les entités publiques et commerciales, et les dommages-intérêts répartis entre les diverses victimes et parties touchées par cette forme de criminalité.

VII. Prévention de la criminalité liée à l'identité

30. Certains États ont signalé des mesures de contrôle et de précaution telles que des limites à la durée de validité, l'exigence du renouvellement, des mesures techniques pour rendre les documents difficiles à falsifier, et des contrôles effectifs de la validité à chaque utilisation. Certains États ont évoqué la nécessité de disposer de systèmes techniques appropriés et de dispenser une formation aux fonctionnaires afin d'améliorer la détection des documents illicites lors de ces contrôles. Les informations fournies par les États ont laissé entrevoir un certain nombre de méthodes qui pourraient être appliquées pour prévenir la criminalité liée à l'identité. Les mesures de sécurité relatives aux documents englobaient à la fois les mesures destinées à rendre les documents plus difficiles à falsifier et celles destinées à protéger les documents authentiques et les systèmes de délivrance contre le vol, le détournement et la délivrance frauduleuse[13]. Les méthodes de validation et de vérification des documents pourraient être renforcées, notamment par l'utilisation de moyens de télécommunications et de bases de données protégés par un codage ou des procédés analogues impliquant la comparaison des informations consignées dans le document et fournies par le titulaire avec des données de référence au moment où le document est utilisé. Des éléments biométriques pourraient servir à rattacher l'identité à des caractéristiques physiques uniques. De façon générale, on pourrait appliquer des mesures de vérification de la sécurité de tous les éléments du système à savoir: la délivrance et le retrait de documents, l'actualisation des documents et des informations; les méthodes relatives à la sécurité de l'information; la validité et le cycle de renouvellement des documents; et l'interopérabilité au niveau mondial des systèmes et des mesures de sécurité.

---

[13] Voir les alinéas a) et b) de l'article 12 à la fois du Protocole relatif à la traite des personnes et du Protocole relatif aux migrants.