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

Distr. générale
2 février 2015
Français
Original: anglais

Doha, 12-19 avril 2015

Point 5 de l'ordre du jour provisoire*
Approches globales et équilibrées visant à prévenir les formes nouvelles et émergentes de criminalité transnationale et à y répondre de façon adéquate

Atelier 3: Renforcement des mesures en matière de prévention du crime et de justice pénale visant à combattre les formes de criminalité en constante évolution, notamment la cybercriminalité et le trafic de biens culturels, enseignements tirés et coopération internationale**

Document d'information

Résumé

Le présent document décrit les aspects communs et spécifiques des mesures en matière de prévention du crime et de justice pénale visant à combattre la cybercriminalité et le trafic de biens culturels, deux exemples notables de formes de criminalité en constante évolution qui ont pris une nouvelle dimension avec la mondialisation et l'essor des technologies de l'information. Alors que les groupes criminels exploitent les possibilités offertes par ces phénomènes, il est nécessaire de prendre des mesures efficaces pour mieux cerner l'ampleur et les racines de ces formes de criminalité et les modes opératoires utilisés, pour mettre au point des stratégies de prévention efficaces, améliorer les échanges d'information et renforcer les cadres nationaux et la coopération internationale entre États Membres.

---

* A/CONF.222/1.

** Le Secrétariat de l'Organisation des Nations Unies tient à remercier les instituts membres du réseau du programme des Nations Unies pour la prévention du crime et la justice pénale, en particulier l'Institut national pour la justice des États-Unis d'Amérique, le Conseil consultatif scientifique et professionnel international, l'Institut coréen de criminologie et l'Institut européen pour la prévention du crime et la lutte contre la délinquance, affilié à l'Organisation des Nations Unies, de l'avoir aidé à préparer et organiser l'Atelier.

Table des matières

I. Introduction

1. Lors des réunions régionales pour l'Asie et le Pacifique, pour l'Asie occidentale et pour l'Afrique, de préparation du treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale, les États Membres ont reconnu qu'il importait d'apporter une réponse globale aux problèmes de la cybercriminalité et du trafic de biens culturels, en constante évolution[1]. Comme c'est le cas pour bon nombre d'autres formes de criminalité, l'efficacité des stratégies de prévention et des mesures de justice pénale visant à combattre ces formes de criminalité en évolution repose sur une base de connaissances détaillées et une bonne compréhension de leurs caractéristiques et des facteurs de nature à les encourager.

2. Le document de travail établi par le Secrétariat sur les approches globales et équilibrées visant à prévenir les formes nouvelles et émergentes de criminalité transnationale et à y répondre de façon adéquate[2] étudiait une typologie à plusieurs niveaux des formes nouvelles et émergentes de criminalité, fondée sur les racines et les vecteurs possibles et les modes opératoires communs. La mondialisation, la proximité de la pauvreté, les conflits et la faiblesse de l'état de droit face aux marchés à forte valeur ajoutée, et l'émergence rapide de nouvelles formes de technologie moderne ont été identifiés comme des racines et des vecteurs possibles de nouvelles formes de criminalité. Le document mettait également en évidence les modifications de la structure des groupes criminels organisés et le recours à la corruption pour faciliter la commission d'infractions comme modes opératoires clefs.

3. Comme c'est le cas d'autres types de criminalité, tels que la piraterie, la maltraitance et l'exploitation des enfants, et le trafic d'espèces de faune et de flore sauvages, les infractions de trafic de biens culturels et de cybercriminalité sont généralement classées dans la catégorie des formes de criminalité émergentes ou en évolution[3]. Comme indiqué dans le document A/CONF.222/8, ces actes ne sont pas toujours entièrement nouveaux, mais peuvent aussi constituer une réémergence de formes de criminalité "conventionnelles", ou l'évolution de nouveaux moyens de commettre des infractions déjà établies.

4. Par exemple, le vol et le trafic de biens culturels à l'échelle nationale existent depuis des siècles. Mais ce n'est que depuis quelques décennies que la communauté internationale cherche à réglementer le commerce de biens culturels et à incriminer spécifiquement le vol d'œuvres d'art et d'antiquités. Dans le même temps, la mondialisation a facilité l'implication croissante de groupes criminels organisés, ce qui a permis l'internationalisation des marchés illicites de biens culturels volés, et donné la possibilité à ces groupes criminels, et peut-être même à des groupes terroristes, de générer des profits non négligeables. De même, des actes liés à l'informatique, notamment l'usage non autorisé de systèmes informatiques et la manipulation de données électroniques, ont été érigés en infraction dans de nombreux pays dès les années 1960. Toutefois, c'est seulement avec l'avènement d'Internet que les technologies mondiales de l'information et de la communication

---

[1] A/CONF.222/RPM.1/1, par. 33 et 35; A/CONF.222/RPM.2/1, par. 38 et 40; et A/CONF.222/RPM.4/1, par. 70.

[2] A/CONF.222/8.

[3] Voir par exemple la résolution 66/181 de l'Assemblée générale, par. 18.

ont commencé à être utilisées pour la commission d'actes criminels de portée transnationale, sous la forme de la cybercriminalité contemporaine.

5. Ainsi, la cybercriminalité et le trafic de biens culturels montrent l'impact que peuvent avoir des racines et des vecteurs tels que la mondialisation et l'émergence de nouvelles formes de technologie sur l'innovation en matière criminelle. Bien que ces deux types de criminalité diffèrent à plus d'un titre, à commencer par l'objet principal de l'infraction, ils présentent un certain nombre de caractéristiques communes.

6. Le trafic de biens culturels est lié au vol, au trafic et à la vente d'objets matériels dont la valeur est liée à leur importance particulière dans le patrimoine culturel. Si l'objet de la cybercriminalité est souvent immatériel, comme des données ou un système informatique, une partie des actes de cybercriminalité sont axés sur le vol et la revente. Par exemple, les infractions informatiques visant à obtenir un gain personnel ou financier ou à faire du tort à autrui peuvent inclure le vol de coordonnées bancaires en ligne ou de numéros de cartes de crédit et leur revente ultérieure à des fins de fraude financière ou de vol. Comme dans le cas du trafic de biens culturels, le vendeur et l'acheteur peuvent très bien se trouver dans des pays différents.

7. En ce qui concerne le degré d'organisation criminelle, les groupes impliqués dans la cybercriminalité peuvent présenter une structure relativement fluide[4]. Cependant, de plus en plus d'éléments indiquent que les groupes organisés selon une structure hiérarchique traditionnelle tirent également parti de la nature immatérielle de la cybercriminalité pour commettre des infractions plus complexes[5]. Ainsi, les sphères du trafic de biens culturels et de la cybercriminalité peuvent se rejoindre au niveau de la vente illicite de biens culturels sur Internet. L'Organisation internationale de police criminelle (INTERPOL), l'Organisation des Nations Unies pour l'éducation, la science et la culture (UNESCO) et le Conseil international des musées ont reconnu, par exemple, que le trafic illicite d'objets culturels sur Internet était un problème très sérieux et qui allait s'aggravant, tant pour les pays "d'origine" que pour les pays de destination[6]. Les Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes[7] s'attaquent à ce problème en recommandant la mise en place de mécanismes devant permettre de signaler des transactions et de contrôler le commerce de biens culturels sur Internet[8].

---

[4] Office des Nations Unies contre la drogue et le crime (ONUDC), *Comprehensive Study on Cybercrime* (Étude approfondie sur le phénomène de la cybercriminalité) (2013, projet), p. 46; et Blythe Bowman Proulx, "Organized criminal involvement in the illicit antiquities trade" (Groupes criminels organisés et trafic illicite d'antiquités), *Trends in Organized Crime*, vol. 14, n° 1 (mars 2011).

[5] Office européen de police, *The Internet Organised Crime Threat Assessment 2014* (Évaluation 2014 de la menace que représente la criminalité organisée sur Internet) (La Haye, 2014), p. 10.

[6] UNESCO, INTERPOL et Conseil international des musées, "Mesures élémentaires concernant les objets culturels mis en vente sur Internet". Disponible à l'adresse http://www.unesco.org/new/fr/culture/themes/illicit-trafficking-of-cultural-property.

[7] Résolution 69/196 de l'Assemblée générale, annexe.

[8] Principes 3 d) et 10.

8. Outre la nature de ces formes de criminalité, et la façon dont elles se rejoignent comme décrit ci-dessus, des points communs peuvent également exister sur le plan de la prévention de la criminalité et de la collecte d'informations à des fins de justice pénale. Les détails sur les tendances et les informations statistiques relatives à ces deux formes de criminalité sont insuffisants. Jusqu'à récemment, une grande partie des informations disponibles au sujet du trafic de biens culturels provenait d'études de cas sur des formes spécifiques de criminalité, comme le vol d'œuvres d'art ou le pillage d'antiquités. Cependant, des efforts ont été déployés pour étoffer les informations disponibles, notamment en collectant, grâce à l'Enquête des Nations Unies sur les tendances de la criminalité et le fonctionnement des systèmes de justice pénale, des statistiques auprès de la police et des tribunaux sur le trafic, le vol, la possession, le recel et l'excavation illicite de biens culturels. Les résultats confirment qu'il faut continuer de collecter des données de manière systématique de façon à obtenir des conclusions représentatives. Cependant, la multitude d'actes différents entrant dans le cadre général de la "cybercriminalité" représente également un défi pour la collecte de données, mais les méthodes impliquant l'utilisation de diverses sources de données semblent prometteuses à cet égard.

9. Bien que l'infraction puisse être commise dans un seul État dans les deux cas, le trafic de biens culturels et la cybercriminalité ont aussi en commun la dimension transnationale, qui fait de la coopération internationale un facteur clef de l'efficacité des mesures de lutte. L'importance cruciale du renforcement de la coopération internationale dans ce domaine a été soulignée dans toutes les réunions régionales préparatoires au treizième Congrès[9]. Selon une estimation, entre 30 % et 70 % des actes de cybercriminalité ont une dimension transnationale[10]. Par ailleurs, le trafic de biens culturels est une infraction de nature principalement transnationale[11]. Les enquêtes relatives à des infractions concernant plusieurs pays nécessitent l'entraide judiciaire la plus large possible lors des enquêtes, des poursuites et des procédures judiciaires, en vue d'accroître l'efficacité et la rapidité des procédures.

10. La coopération internationale se trouve facilitée lorsque les cadres juridiques nationaux érigent en infraction la même conduite sous-jacente. Dans le cas du trafic de biens culturels, les infractions spécifiques peuvent inclure le trafic, l'exportation et l'importation illicites et le vol de biens culturels, ainsi que le pillage et la fouille illicite de sites archéologiques et culturels[12]. Dans le cas de la cybercriminalité, des dispositions de droit pénal spécifiques sont généralement nécessaires pour incriminer les actes ciblant des données ou des systèmes informatiques, tels que l'accès illégal à ces systèmes ou données.

11. Enfin, les mesures de lutte contre ces deux formes de criminalité sont les plus efficaces lorsqu'elles incluent une approche multipartite. Une très large partie de l'infrastructure d'Internet, sur laquelle reposent de nombreuses formes de cybercriminalité et de trafic de biens culturels, appartient au secteur privé, qui

---

[9] A/CONF.222/RPM.1/1, par. 34; A/CONF.222/RPM.2/1, par. 40; A/CONF.222/RPM.3/1, par. 61; et A/CONF.222/RPM.4/1, par. 71.

[10] ONUDC, *Comprehensive Study on Cybercrime* (Étude approfondie sur le phénomène de la cybercriminalité), p. 183.

[11] CTOC/COP/2010/12, par. 33.

[12] Voir le Principe 16 des Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes.

l'exploite également. Les objets de valeur culturelle peuvent appartenir à des propriétaires très divers, dont des États, des particuliers, des musées, des fonds et autres associations non gouvernementales. La participation de toutes les parties concernées, notamment au moyen de partenariats public-privé, est essentielle pour faire connaître le risque d'infractions et promouvoir de bonnes pratiques en matière de prévention de la criminalité, ainsi que pour faciliter les enquêtes et permettre aux victimes d'obtenir une indemnisation ou une réparation.

12. Le présent document d'information, qui s'appuie sur le cadre établi dans le document A/CONF.222/8, vise à illustrer les leçons tirées de l'expérience et les modalités de la coopération internationale relatives aux formes de criminalité en évolution que sont la cybercriminalité et le trafic de biens culturels. Il examine la base de connaissances concernant chaque type de criminalité, ainsi que les difficultés rencontrées et les pratiques mises en œuvre dans le domaine des législations nationales, les modes d'enquête et les formes de coopération internationale. Des points de départ possibles pour la prévention du crime sont mis en évidence, le cas échéant. Enfin, ce document étudie les mesures qui peuvent être prises tant par les États que par l'ensemble de la communauté internationale pour renforcer l'action mondiale en matière de prévention du crime et de justice pénale.

II. Cybercriminalité

A. Cerner le problème

13. En 1994, il était noté dans le *Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique* que "la criminalité informatique était potentiellement aussi vaste que l'étaient les systèmes de télécommunication internationaux"[13]. S'il n'est peut-être pas surprenant que le mot "Internet" ne soit employé qu'une seule fois dans ce manuel, et que le terme "cybercriminalité" n'y apparaisse pas du tout, ses conclusions sont toujours d'actualité. Si le manuel mettait l'accent sur la notion de "criminalité informatique", il est largement reconnu aujourd'hui que la cybercriminalité repose en effet sur des technologies mondiales de l'information et de la communication, notamment Internet, pour commettre des infractions d'ampleur transnationale.

14. Avec l'évolution de la terminologie, des universités ont entrepris de définir le terme "cybercriminalité"[14]. Une approche moderne consiste à reconnaître que la cybercriminalité n'est pas nécessairement un terme technique juridique, mais plutôt un terme global désignant l'ensemble des actes commis à l'encontre ou à l'aide de données ou de systèmes informatiques. D'autres démarches se concentrent sur les infractions concernant des données informatiques, ou sur l'utilisation de ressources informatiques à des fins illégales[15].

---

[13] *Manuel des Nations Unies sur la prévention et la répression de la criminalité informatique*, Revue internationale de politique criminelle, Série M, n^{os} 43 et 44 (publication des Nations Unies, numéro de vente: F.94.IV.5), par. 12.

[14] Voir par exemple David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cybercriminalité: la transformation de la criminalité à l'ère de l'informatique) (Cambridge, Polity Press, 2007).

[15] Voir par exemple l'Accord de coopération de la Communauté d'États indépendants en matière de lutte contre les infractions dans le domaine informatique (2001).

15. Les agissements qui entrent généralement dans la catégorie de la cybercriminalité incluent ceux dans le cadre desquels des données ou des systèmes informatiques sont l'objet même de l'infraction, ainsi que ceux dans le cadre desquels des ordinateurs ou des systèmes informatiques font partie intégrante du mode opératoire de l'infraction. La première catégorie couvre par exemple les infractions à l'encontre de la confidentialité, de l'intégrité et de la disponibilité des données ou systèmes informatiques, telles que l'accès illégal à ces données ou systèmes (parfois appelées actes "principaux" de cybercriminalité). La seconde catégorie couvre l'usage de données ou de systèmes informatiques à des fins de fraude, de vol, ou pour faire du tort à autrui, ainsi que les infractions informatiques et liées au contenu d'Internet, y compris l'incitation à la haine, la pornographie enfantine, les infractions liées à l'identité et la vente en ligne de biens illicites[16].

16. De manière générale, toutefois, la frontière entre cybercriminalité et criminalité classique est de plus en plus floue. Alors que les appareils électroniques et la connectivité globale sont de plus en plus omniprésents dans notre vie quotidienne, les preuves électroniques telles que les SMS, les courriers électroniques et les données relatives à la navigation Internet et aux réseaux sociaux, deviennent la norme dans de nombreuses enquêtes criminelles classiques. Les outils d'investigation numérique et les demandes envoyées aux fournisseurs de services électroniques dans de tels cas, ainsi que bon nombre de difficultés rencontrées et de bonnes pratiques utilisées dans les enquêtes, sont souvent les mêmes que dans les affaires de cybercriminalité. C'est pourquoi, bien que le présent document se concentre sur des actes qui sont généralement considérés comme relevant de la cybercriminalité, plusieurs de ses constatations et conclusions peuvent s'appliquer plus largement aux preuves électroniques en général.

17. Un des principaux facteurs sous-jacents de la cybercriminalité contemporaine comme de l'essor des preuves électroniques est la hausse de la connectivité électronique mondiale. On compte aujourd'hui près de trois milliards d'internautes, ce qui représente environ 40 % de la population mondiale. La plupart d'entre eux accèdent à Internet par un service mobile à large bande, ce type de service étant accessible à environ 32 % de la population mondiale, un chiffre presque quatre fois plus élevé qu'en 2009[17]. Le nombre d'appareils connectés à des réseaux à protocole Internet devrait représenter près du double de la population mondiale d'ici à 2018[18].

18. Si cette croissance rapide d'Internet et de l'informatique a permis la croissance économique et un meilleur accès à des services aussi essentiels que l'éducation, les soins de santé et la cybergouvernance, elle a également ouvert de nouvelles possibilités d'activités criminelles. Les outils de la cybercriminalité tels que les "réseaux zombies", par exemple, peuvent être composés de réseaux mondiaux comptant plusieurs dizaines, voire centaines de milliers, d'appareils victimes, tous infectés par un logiciel malveillant qui peut être contrôlé à distance par les délinquants. Les réseaux sociaux peuvent être utilisés à des fins de harcèlement criminel, d'incitation à la haine, de menaces de violence, d'extorsion ou de

---

[16] ONUDC, *Comprehensive Study on Cybercrime* (Étude approfondie sur le phénomène de la cybercriminalité), p. 16.

[17] Union internationale des télécommunications, "Le monde en 2014: données et chiffres concernant les TIC" (Genève, 2014).

[18] Cisco, "The zettabyte era: trends and analysis" (L'ère du zettabit: tendances et analyse), Cisco Visual Networking Index (San José, Californie, 2014).

diffusion de données privées à l'échelle mondiale et en quelques secondes. Les délinquants cherchant également à viser l'Internet des objets, le potentiel global d'activité criminelle pourrait encore augmenter.

19. En plus de la nature mondiale de ce problème, on a observé au cours des 10 dernières années des cycles dans le niveau d'anonymat offert par Internet, et son utilisation conséquente dans des activités criminelles. À son commencement, on pensait généralement qu'Internet était largement anonyme, au moins dans la mesure où les utilisateurs ne comprenaient pas qu'il était techniquement possible de remonter les traces d'activité en ligne jusqu'aux individus. Cependant, au cours des dernières années, les systèmes de justice pénale se sont familiarisés avec les notions d'adresses IP et de journaux de connexion, et ont pris l'habitude d'émettre des ordonnances pour obtenir des données auprès des fournisseurs de services électroniques. Par conséquent, les traces électroniques laissées par les internautes sont de plus en plus facilement accessibles aux enquêteurs, même si l'obtention de données Internet peut demander beaucoup de temps et d'efforts. De même, les progrès des outils d'investigation numérique, dont les périphériques prêts à brancher, simples à utiliser, ont facilité les analyses de routine des données stockées sur des appareils numériques tels que les ordinateurs et les smartphones.

20. La technologie est en progrès constant, et les outils de criminalistique et les méthodes d'enquête relatives à la cybercriminalité d'aujourd'hui font face à des défis qu'il aurait été impossible de prévoir il y a 10 ans. Par exemple, des logiciels gratuits et largement accessibles permettent de crypter en 256 bits des fichiers individuels ou des dispositifs entiers de stockage des données. Sans mot de passe ou clef, les données ainsi cryptées sont pratiquement inaccessibles aux organes de détection et de répression. Le cryptage 2 048 bits, encore plus complexe, représente à ce jour une norme théoriquement inviolable. De nouveaux réseaux décentralisés d'anonymisation, qui forment ce que l'on appelle parfois le "web obscur", fonctionnent parallèlement à l'Internet conventionnel. Des services tels que The Onion Router (Tor) compliquent la tâche de nombreux organes de détection et de répression qui cherchent à déterminer l'origine de communications électroniques, ou l'identité de sites offrant des "services cachés". Ces services cachés peuvent être utilisés pour héberger anonymement des marchés illicites en ligne de drogues, d'armes, ou de pornographie enfantine. Certains de ces réseaux permettent également le stockage décentralisé de données cryptées dans des nœuds de réseaux connectés. Les documents ou images électroniques ainsi stockés sont eux aussi pratiquement inaccessibles aux organes de détection et de répression. Ces technologies ont des répercussions profondes pour les organes de détection et de répression, et posent la question de savoir comment l'action de répression peut suivre le rythme de l'innovation en matière de cybercriminalité.

B. Mesurer la cybercriminalité

21. Une méthode de mesure des nouvelles formes et dimensions de la criminalité, y compris la cybercriminalité, s'appuie sur la combinaison de plusieurs mesures, telles que les informations sur les auteurs d'infractions, les informations sur les flux au sein des marchés illicites et les informations sur le nombre d'actes criminels, de préjudices et de pertes et les flux financiers illicites qui en découlent. Pour la cybercriminalité, plusieurs sources de données peuvent être utilisées à cet égard, dont les statistiques sur la criminalité recueillies par la police, les enquêtes menées

auprès de la population et des entreprises, les signalements des victimes, et les renseignements informatisés sur la cybersécurité. L'exploration des URL et la reprise de "réseaux zombies" constituent également des techniques supplémentaires.

22. Même si les statistiques recueillies par la police sur la cybercriminalité ne doivent pas être négligées, il est clair qu'elles sont très limitées, car la plupart des cas de victimisation ne sont pas signalés à la police. Dans une enquête menée auprès de 20 000 internautes dans 24 pays, seuls 21 % des répondants qui ont déclaré avoir été victimes de la cybercriminalité ont signalé cet acte à la police[19]. À l'échelle mondiale, les organes de détection et de répression peuvent utiliser des méthodes statistiques et des démarches différentes, ce qui rend les comparaisons internationales difficiles. De plus, le niveau global d'actes de cybercriminalité enregistrés par la police est étroitement lié au nombre d'unités de police spécialisée, ce qui donne à penser que les statistiques reflètent davantage les activités d'enquête de la police que la victimisation sous-jacente due à la criminalité[20].

23. Les enquêtes de victimisation menées auprès de particuliers ou d'entreprises constituent une autre source d'information importante. Elles donnent à penser qu'au sein de la population générale, le risque d'être victime de la cybercriminalité est beaucoup plus élevé que pour les formes de criminalité "classiques". Les taux de victimisation pour la fraude en ligne à la carte de crédit, l'usurpation d'identité, la réponse à une tentative d'hameçonnage et l'accès non autorisé à un compte de messagerie électronique varient entre 1 % et 17 % de la population en ligne dans 21 pays à travers le monde, contre moins de 5 % pour les cambriolages, les vols qualifiés et les vols de véhicules automobiles dans les mêmes pays[21]. Les entreprises du secteur privé signalent des taux de victimisation similaires: entre 2 % et 16 % en Europe, par exemple, pour des actes tels que la violation de données par intrusion ou l'hameçonnage[22]. Une étude a montré qu'en 2012, le nombre de victimes d'usurpation d'identité avait augmenté de plus d'un million, et que les auteurs de ces actes avaient volé plus de 21 milliards de dollars des États-Unis, la somme la plus élevée depuis 2009, quoique largement inférieure aux pertes de 2004, estimées à 47 milliards de dollars[23].

24. Les données issues des enquêtes qui contiennent des informations sur les pertes financières résultant de la cybercriminalité peuvent être utilisées pour établir des estimations de son impact. Dans une enquête, des consommateurs victimes d'actes de cybercriminalité dans 24 pays à travers le monde ont signalé des pertes directes moyennes comprises entre 50 et 850 dollars sur une année[24]. Grâce aux données de plusieurs enquêtes, une autre étude a estimé que les coûts directs et indirects (y compris le coût de la sécurité) de plusieurs formes de cybercriminalité,

---

[19] Symantec, "Norton Cybercrime Report" (Rapport de Norton sur la cybercriminalité), 2012. Disponible à l'adresse http://us.norton.com/cybercrimereport.

[20] ONUDC, *Comprehensive Study on Cybercrime* (Étude approfondie sur le phénomène de la cybercriminalité), annexe 2.

[21] Données d'enquête fournies par Symantec.

[22] Eurostat, Statistiques sur la société de l'information, Enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises, 2011. Disponible à l'adresse http://ec.europa.eu/eurostat/web/information-society/data/database.

[23] Javelin Strategy and Research, "2013 Identity Fraud Report: Data Breaches becoming a treasure trove for fraudsters" (Rapport 2013 sur l'usurpation d'identité: la violation de données devient une manne pour les escrocs). Disponible à l'adresse www.javelinstrategy.com/brochure/276.

[24] Données d'enquête fournies par Symantec.

dont la fraude bancaire en ligne, la fraude aux cartes de paiement en ligne et la fraude aux avances de frais, s'élevaient à plusieurs centaines, voire milliers, de millions de dollars dans le monde chaque année[25].

25. L'analyse des marchés de la cybercriminalité offre également des possibilités d'évaluer la nature et l'ampleur de certaines de ses formes. L'une des méthodes se concentre sur l'analyse de forums en ligne qui servent de réseaux sociaux aux délinquants pour la vente et l'achat de biens sociaux et le partage d'informations de nature criminelle.

26. Une étude réalisée en 2011 a utilisé les données provenant de six forums clandestins, qui contenaient plus de 2,5 millions de contributions et 900 000 messages privés envoyés par plus de 100 000 utilisateurs. Les coordonnées bancaires et de cartes de crédit ainsi que les instruments utilisés pour la fraude faisaient partie des marchandises les plus couramment échangées[26]. Il ressort d'une analyse récente des fils de discussion de 13 forums Internet que des listes de coordonnées de cartes de crédit volées sont proposées en ligne pour un prix moyen d'environ 100 dollars, et que des outils criminels tels que les copieurs de carte peuvent être acquis pour environ 2 400 dollars[27]. Les nouvelles techniques de recherche permettent également d'explorer automatiquement les services cachés du réseau Tor, ce qui peut faciliter le recensement et la catégorisation systématiques du nombre et du type de sites du Web obscur liés à des domaines tels que la vente de drogues illicites, d'armes ou d'outils de cybercriminalité, et à la pornographie enfantine[28].

27. Enfin, la typologie des auteurs d'infractions aide à comprendre la nature et le mode opératoire des organisations criminelles auxquelles ils appartiennent. Il n'y a probablement pas de "profil" standard dans ce domaine. Il se peut qu'un nombre relativement faible de programmeurs et de pirates informatiques hautement qualifiés mènent l'innovation en matière cybercriminelle et mettent leurs talents au service de la criminalité. Cependant, du fait de la facilité d'accès aux logiciels malveillants ou d'exploitation, de nombreux délinquants n'ont plus besoin de connaissances approfondies. De plus en plus souvent, la cybercriminalité peut aussi avoir besoin d'un grand nombre de "pions" de bas niveau. Dans le cadre d'une opération récente de fraude aux cartes de paiement prépayées, un groupe criminel organisé a recruté des centaines de personnes dans 26 pays, afin d'effectuer plus de 40 000 retraits simultanés à des distributeurs automatiques en deux occasions, pour un butin estimé

---

[25] Ross Anderson et autres, "Measuring the cost of cybercrime" (Mesurer le coût de la cybercriminalité), dans *The Economics of Information Security and Privacy*, Rainer Böhme (dir. publ.) (Springer Berlin Heidelberg, Berlin, 2013).

[26] Marti Motoyama et autres, "An analysis of underground forums" (Une analyse des forums clandestins), dans *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2011).

[27] Thomas Holt et Olga Smirnova, "Examining the structure, organization, and processes of the international market for stolen data" (Examiner la structure, l'organisation et les processus du marché international des données volées), étude réalisée pour l'Institut national pour la justice, Rockville, Maryland, États-Unis d'Amérique, mars 2014.

[28] Martijn Spitters et autres, "Towards a comprehensive insight into the thematic organization of the ToR hidden services" (Vers un aperçu global de l'organisation thématique des services cachés de ToR), étude présentée à la Conférence conjointe de l'IEEE sur le renseignement et la sécurité informatique, La Haye, septembre 2014.

à 45 millions de dollars[29]. Même si plus de 80 % des actes de cybercriminalité relèvent de la criminalité organisée[30], il est clair que la diversité des structures des groupes, y compris des associations criminelles plus souples, représente un défi pour toute tentative de classification des cybercriminels.

C. Prévenir et combattre la cybercriminalité

28. Les informations sur la nature et l'ampleur de la cybercriminalité sont des éléments essentiels dans la conception de stratégies efficaces de prévention et d'enquête. Les stratégies de sensibilisation conçues pour prévenir la fraude à la consommation en ligne, par exemple, peuvent nécessiter une approche différente de celles visant la protection de l'enfance en ligne. À cet égard, les réunions régionales pour l'Asie et le Pacifique, pour l'Asie occidentale et pour l'Afrique, de préparation du treizième Congrès ont recommandé l'élaboration d'outils et de programmes susceptibles de faciliter la sensibilisation et la prévention en matière de cybercriminalité. Les informations sur les menaces et les tendances dans ce domaine peuvent également servir de base pour les enquêtes. Les enquêtes concernant la vente de drogues illicites sur Internet, par exemple, nécessitent des compétences et des techniques différentes de celles utilisées pour l'examen criminalistique d'appareils informatiques. Les données disponibles sur la cybercriminalité peuvent aider à cibler les efforts de façon à lutter contre les tendances émergentes, mais la diversité des actes de cybercriminalité exige que les pays développent leurs capacités à travers toute une gamme de mesures de prévention et d'enquête.

29. En plus des capacités en matière de mesure de la cybercriminalité, des mesures doivent être prises à l'échelle nationale dans les domaines des cadres législatifs et de politique générale, y compris sur les thèmes suivants: incrimination et règles de procédure; capacités de détection et de répression et capacités du système de justice pénale en matière d'enquêtes sur la cybercriminalité, d'investigation numérique et de gestion des preuves électroniques; mécanismes de coopération internationale en matière pénale; et prévention de la cybercriminalité.

30. Les politiques, stratégies et dispositions législatives nationales relatives à la cybercriminalité constituent un point de départ essentiel pour définir le cadre et les priorités de la lutte contre ce phénomène. Le répertoire en ligne de l'ONUDC sur la cybercriminalité (qui doit être lancé en 2015) contiendra des détails sur les stratégies nationales répertoriées dans une cinquantaine de pays, qui couvrent des domaines tels que la sensibilisation à la cybercriminalité, la coopération internationale, les capacités de détection et de répression, la législation, la prévention et les partenariats public-privé. La législation nationale sur la cybercriminalité couvre aussi fréquemment plusieurs domaines comme l'incrimination, les pouvoirs d'enquête, la compétence, les preuves électroniques et la coopération internationale. L'examen de ces lois montre que la cybercriminalité est incriminée grâce à une combinaison d'infractions propres à l'informatique et

---

[29] INTERPOL, "Un réseau criminel se livrant à des fraudes aux cartes bancaires démantelé avec l'appui d'INTERPOL", 30 avril 2014. Disponible à l'adresse http://www.interpol.int/fr/Internet/Centre-des-médias/Nouvelles/2014/N2014-074.

[30] BAE Systems Detica et John Grieve Centre for Policing and Community Safety, *Organised Crime in the Digital Age* (La criminalité organisée à l'ère numérique) (Université métropolitaine de Londres, 2012).

d'infractions générales. Les actes "principaux" de cybercriminalité tels que l'accès non autorisé à des données ou des systèmes informatiques peuvent être incriminés par une disposition juridique spécifique, tandis que les agissements liés à l'utilisation d'ordinateurs visant à réaliser un gain personnel ou financier ou à faire du tort à autrui constituent plus souvent des infractions générales (non spécifiques à l'informatique)[31].

31. Dans certains cas, les cadres juridiques nationaux sont adoptés en application d'un instrument multilatéral, qui peut être contraignant ou non, ou s'en inspirent. On trouve parmi ces instruments l'Accord de coopération de la Communauté d'États indépendants en matière de lutte contre les infractions dans le domaine informatique, l'Accord de l'Organisation de Shanghai pour la coopération dans le domaine de la sécurité internationale de l'information, la Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information, la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel, la Convention sur la cybercriminalité du Conseil de l'Europe, et la Directive 2013/40/UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information. En ce qui concerne la possibilité d'élaborer de nouveaux cadres multilatéraux, la Réunion régionale pour l'Afrique préparatoire au treizième Congrès a recommandé que les États envisagent d'élaborer une convention sur la cybercriminalité dans le contexte du treizième Congrès.

32. Outre des dispositions relatives à l'incrimination et aux règles de procédure, les instruments existants peuvent aussi prévoir des mécanismes de coopération internationale dans le cadre d'enquêtes et de poursuites transfrontières relatives à la cybercriminalité. Ce domaine représente un défi croissant pour les autorités de détection et de répression. Avec l'apparition de l'informatique en nuage et du partage et du stockage de données de pair à pair, la localisation de données informatiques particulières peut en théorie être déterminée à un instant précis, mais il peut exister de multiples copies de ces données, réparties entre divers appareils en divers lieux, et qui peuvent être transférées d'un lieu à un autre en quelques secondes.

33. Certains fournisseurs de services de stockage de données, comme les fournisseurs de services électroniques privés ou de services en nuage, peuvent être légalement tenus de conserver des copies des données pendant un certain temps, et communiqueront généralement ces données aux autorités de détection et de répression sur ordonnance judiciaire ou dans le cadre de toute autre procédure juridique appropriée. Cependant, lorsque le fournisseur ou les données se trouvent hors du pays où l'enquête est menée, il est souvent nécessaire de lancer une procédure d'entraide judiciaire formelle – et laborieuse – entre les États. Dans le cas d'autres modes de stockage des données, par exemple par des particuliers sur un réseau informatique de pair à pair, les données, qui peuvent de toute façon être difficiles à identifier, sont souvent cryptées. Il peut alors être nécessaire de prendre des mesures coercitives contre une personne pour sécuriser les données et obtenir leur divulgation.

---

[31] ONUDC, *Comprehensive Study on Cybercrime* (Étude approfondie sur le phénomène de la cybercriminalité), p. 78.

34. Des discussions sont en cours à l'échelle internationale au sujet du système actuel, essentiellement territorial, qui prévaut pour les enquêtes transnationales en matière de cybercriminalité et l'accès aux données se pratique déjà à plusieurs niveaux[32]. Certains instruments multilatéraux existants établissent des mécanismes qui visent à faciliter l'accès aux données pour les organes de détection et de répression, comme des points de contact disponibles 24 heures sur 24 pendant les enquêtes, la protection rapide des données, l'accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public, et les demandes urgentes d'entraide. Dans la pratique, il est clair que malgré ces mécanismes, de nombreuses autorités de détection et de répression ont des difficultés à accéder rapidement à des données extraterritoriales lors d'enquêtes sur la cybercriminalité. Dans le même temps, le respect des droits de l'homme, de l'état de droit et des garanties relatives à la vie privée doit être suffisant pour que l'accès aux données par des organes de détection et de répression soit défini, prévisible, proportionné et soumis à un contrôle approprié.

35. Des innovations telles que l'inclusion d'un module sur les preuves numériques lors de la refonte du Rédacteur de requêtes d'entraide judiciaire de l'Office des Nations Unies contre la drogue et le crime (ONUDC) pourraient contribuer à rationaliser les processus d'entraide judiciaire concernant les preuves électroniques. Cependant, en parallèle, les autorités de détection et de répression devront trouver des façons toujours plus innovantes de collaborer dans les enquêtes transnationales sur la cybercriminalité. Le fait que des entités telles que le Complexe mondial INTERPOL pour l'innovation et le Centre européen de lutte contre la cybercriminalité de l'Office européen de police (Europol) participent à la coordination des enquêtes transnationales et apportent leur soutien, notamment en facilitant le partage d'informations entre les autorités nationales de détection et de répression, pourrait se révéler particulièrement important à cet égard. D'autres forums et initiatives, comme la Conférence mondiale sur le cyberespace, ont également fourni aux pays une occasion d'envisager des mesures innovantes dans le domaine de la coopération internationale contre la cybercriminalité.

36. Les partenariats de prévention et de lutte contre la cybercriminalité, au niveau multilatéral ou national, doivent également faire appel au secteur privé. Les fournisseurs d'accès à Internet et les hébergeurs peuvent jouer un rôle déterminant dans la prévention de la cybercriminalité. Ils peuvent conserver des journaux de connexion qui peuvent être utilisés dans les enquêtes criminelles, aider les clients à adopter des pratiques d'utilisation sûres d'Internet et à repérer les ordinateurs compromis, bloquer certains types de contenus malveillants, et de manière générale, maintenir un environnement de communication sécurisé pour leurs clients. Il existe un certain nombre de modèles de partenariats public-privé, par exemple entre les autorités de détection et de répression et les fournisseurs de services électroniques. Nombre d'entre eux sont fondés sur le partage d'informations reposant sur des

---

[32] Voir par exemple Conseil de l'Europe, "Rapport d'évaluation du Comité de la Convention Cybercriminalité: les dispositions de la Convention de Budapest sur la cybercriminalité concernant l'entraide", document T-CY(2013)17rev, et "Accès transfrontalier aux données et compétence: options concernant l'action future du Comité de la Convention Cybercriminalité", document T-CY(2014)16, et Albert Rees, "International cooperation in cybercrime investigations" (Coopération internationale dans les enquêtes sur la cybercriminalité), présentation préparée pour l'atelier régional de l'Organisation des États américains sur la cybercriminalité, avril 2007.

règles claires, la confiance, un nombre de membres restreint, des bénéfices mutuels et la rapidité de réaction. Dans certains cas, des associations professionnelles, comme la Cyber Security Research Alliance, constituent des plates-formes de collaboration entre les entreprises et les gouvernements dans les domaines de la cybersécurité et de la cybercriminalité.

37. Enfin, le renforcement des capacités nationales dans les domaines de la détection et la répression et de la justice pénale est capital. La majorité des pays ont commencé à mettre en place des structures spécialisées chargées d'enquêter sur la cybercriminalité et les infractions pour lesquelles il existe des éléments de preuve électroniques, mais souvent, ces structures manquent de ressources et de capacités. Les preuves numériques étant de plus en plus présentes dans les enquêtes sur des infractions classiques, les autorités de détection et de répression doivent établir des distinctions claires entre les enquêteurs travaillant sur des affaires de cybercriminalité et le personnel des laboratoires de criminalistique numérique et définir des flux de travail distincts les concernant. Les agents de première ligne pourraient également devoir acquérir des compétences de base, comme la capacité de produire une copie-image fiable d'un appareil de stockage électronique.

38. Les nouvelles évolutions technologiques telles que les réseaux d'anonymisation, le cryptage de haut niveau et les monnaies virtuelles, devenant de plus en plus courantes dans les infractions de cybercriminalité, les enquêteurs devront également adopter de nouvelles stratégies. Les autorités de détection et de répression pourraient par exemple chercher à renforcer les partenariats avec des groupes de recherche universitaire qui cherchent à développer de nouvelles méthodes dans des domaines tels que la typologie et l'analyse des opérations impliquant des monnaies virtuelles[33]. Les enquêteurs devront peut-être également étudier la façon dont les techniques d'enquête spéciales, comme la surveillance, les opérations d'infiltration, le recours à des informateurs et à des livraisons surveillées dans le cas de la vente en ligne de marchandises illicites, pourraient être utilisées parallèlement aux enquêtes sur Internet et aux techniques de criminalistique numérique. Dans l'ensemble, il est clair que le renforcement des capacités des agents de détection et de répression et de la justice pénale aux fins de la lutte contre la cybercriminalité sera un processus permanent et continu, car la technologie et l'innovation en matière criminelle évoluent rapidement.

III. Trafic de biens culturels

A. Définir le problème

39. La protection des biens culturels est considérée comme l'un des principaux défis que doivent relever les politiques de justice pénale actuelles. Ces biens en sont venus à être perçus comme un atout non seulement pour les "pays d'origine", mais aussi pour l'ensemble de l'humanité; ils méritent d'être protégés et préservés pour leur intérêt historique, leur contribution à la formation de l'identité culturelle et le

---

[33] Voir par exemple Sarah Meiklejohn et autres, "A fistful of bitcoins: characterizing payments among men with no names" (Une poignée de bitcoins: typologie des paiements d'hommes sans nom), dans *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2013).

rôle qu'ils jouent dans les pratiques sociales. D'où l'attention croissante que l'ONU et de nombreuses autres organisations internationales portent à ce phénomène, et la volonté qu'ont les États d'élaborer et de mettre en œuvre des instruments juridiques internationaux propres à protéger ces biens.

40. La conduite fondamentale que l'on pourrait associer au trafic de biens culturels peut être plus simple que celle des cybercriminels, mais il est très difficile de définir la portée et l'ampleur du problème. Cette difficulté est inhérente à de nombreux types d'activités criminelles organisées et tient notamment à la complexité des opérations illégales, au manque de moyens et de prise de conscience des services de détection et de répression, ainsi qu'à la corruption. En outre, la proximité qui existe entre les activités illégales d'exportation de biens culturels volés, certains acteurs du marché légal de l'art et des antiquités et les méthodes de fonctionnement de ce dernier dans de nombreux pays fait qu'il est nécessaire d'intensifier l'action menée. Les difficultés sont exacerbées lorsqu'il s'agit de biens culturels issus de fouilles illicites pratiquées sur des sites archéologiques, car il peut être extrêmement difficile de déterminer l'origine de ces objets.

41. Des efforts ont été faits pour recueillir des données sur le trafic de biens culturels et déterminer les méthodes utilisées par les groupes criminels. En 2009, par exemple, une étude a utilisé les données du système WITS de la Banque mondiale, qui comprend des données sur des objets vieux de plus de 100 ans, pour élaborer des modèles empiriques expliquant la contrebande d'objets d'art et d'antiquités[34]. Cette étude a révélé l'existence d'un lien étroit entre la corruption et la probabilité de sous-déclaration d'exportations d'antiquités, puissant indicateur de contrebande.

42. Une autre approche a consisté à tenter de cartographier et mesurer les marchés illicites des biens culturels. Certaines études ont examiné la demande des marchés, se concentrant sur la vente d'objets d'art et d'antiquités dans les maisons d'enchères et tentant d'établir l'origine et l'historique de propriété de ces pièces. En 2002, par exemple, une étude a examiné plus de 18 000 pièces de poterie grecque vendues dans des maisons d'enchères aux États-Unis d'Amérique et au Royaume-Uni de Grande-Bretagne et d'Irlande du Nord entre 1954 et 1998, pour constater qu'entre 80 % et 90 % de ces pièces n'avaient pas de provenance (la chaîne de propriété légitime ne pouvait être remontée jusqu'à la découverte initiale)[35]. L'absence de provenance n'est pas en soi une preuve de contrebande, mais elle représente un facteur de risque important. D'autres études de marchés illicites se concentrent sur l'offre, le plus souvent en examinant et en documentant les sites archéologiques pillés. Certaines de ces études suivent les méthodologies traditionnelles des sciences sociales et comportementales, y compris la recherche sur le terrain dans le but de documenter l'état de sites archéologiques de certains pays. Depuis peu, l'utilisation de satellites commerciaux très puissants permet de surveiller plus fréquemment et à grande échelle des sites pour y déceler des signes de pillage. En 2008, par exemple,

---

[34] Raymond Fisman et Shang-Jin Wei, "The Smuggling of Art, and the Art of Smuggling: Uncovering the Illicit Trade in Cultural Property and Antiques", *American Economic Journal: Applied Economics*, vol. 1, n° 3 (juillet 2009), p. 82 à 96.

[35] Vinnie Nørskov, *Greek Vases in New Contexts* (Aarhus (Danemark), Aarhus University Press, 2002).

plusieurs études ont utilisé l'imagerie numérique pour documenter l'étendue du pillage de sites archéologiques iraquiens[36].

43. Certaines études ont également examiné les différentes étapes de la chaîne d'approvisionnement illicite en biens culturels objets d'un trafic. Certaines se sont concentrées sur les auteurs de pillages de sites archéologiques, telle une étude qui, en 2005, a examiné le cas de 400 de ces personnes au Belize, concluant que le principal facteur de motivation de ces auteurs était la subsistance économique, plutôt que des intentions malveillantes[37]. En 2003 et 2004, une autre étude, consacrée au pillage perpétré en Irak, a révélé une motivation économique similaire, notant également la présence de formes plus organisées de criminalité, avec un contrôle de l'accès aux sites et l'assassinat de douaniers iraquiens qui tentaient de s'opposer au pillage[38]. Plus récemment, l'étude empirique d'un réseau de trafic de statues a utilisé les entretiens oraux menés lors de travaux de criminologie ethnographique effectués au Cambodge et en Thaïlande, se penchant également sur le niveau d'organisation des activités illicites connexes[39].

44. Certaines études ont débattu de la présence du crime organisé, transnational ou non, sur les marchés illicites de biens culturels. L'une d'elles, après avoir réalisé une métaanalyse d'études publiées antérieurement sur le trafic de biens culturels, a conclu qu'il valait mieux cartographier la façon dont ce commerce se déroule et déterminer les rôles et les relations des différents auteurs dans chaque réseau que supposer que tous les types de trafic de biens culturels relèvent du crime organisé[40]. Une autre a appliqué le paradigme des réseaux pour expliquer la structure relativement souple du commerce illicite de biens culturels, encourageant à mener d'autres études sur la structure organisationnelle de ce type de trafic[41]. Une autre, enfin, a cartographié la chaîne des coauteurs d'un trafic, analysant leur rôle, leurs relations et leur conduite, qui est, en partie, hiérarchiquement structurée[42].

B. Mesures prises pour combattre le trafic des biens culturels

45. Plusieurs instruments internationaux ont été adoptés pour combattre le trafic de biens culturels. Prévenir et sanctionner le préjudice infligé aux biens culturels pendant les guerres a été le premier objectif de la Convention pour la protection des biens culturels en cas de conflit armé et de ses protocoles additionnels. D'autres

---

[36] Voir Elizabeth Stone, "Patterns of looting in southern Iraq", *Antiquity*, vol. 82, n° 315 (mars 2008), p. 125 à 138.

[37] David Matsuda, "Subsistence Diggers", dans *Who Owns the Past? Cultural Policy, Cultural Property, and the Law*, Kate Fitz Gibbon, coll. (New Brunswick, New Jersey, Rutgers University Press, 2005), p. 255 à 268.

[38] Joanne Farchakh-Bajjaly, "Who are the Looters at Archaeological Sites in Iraq?", dans *Antiquities Under Siege: Cultural Heritage Protection After the Iraq War*, Lawrence Rothfield, coll. (Washington, AltaMira Press, 2008), p. 49 à 56.

[39] Simon Mackenzie et Tess Davis, "Temple looting in Cambodia: anatomy of a statue trafficking network", *British Journal of Criminology*, vol. 54, n° 5 (septembre 2014), p. 722 à 740.

[40] Jessica Dietzler, "On 'organized crime' in the illicit antiquities trade: moving beyond the definitional debate", *Trends in Organized Crime*, vol. 16, n° 3 (septembre 2013), p. 329 à 342.

[41] Peter B. Campbell, "The illicit antiquities trade as a transnational criminal network: characterizing and anticipating trafficking of cultural heritage", *International Journal of Cultural Property*, vol. 20, n° 2 (mai 2013), p. 113 à 153.

[42] Mackenzie et Davis, "Temple looting in Cambodia: anatomy of a statue trafficking network".

instruments internationaux traitent de l'importation, de l'exportation et du transfert de propriété illicites de biens culturels dans tout type de circonstance. Ce sont notamment la Convention concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels et la Convention sur les biens culturels volés ou illicitement exportés. La volonté qu'a la communauté internationale de sauvegarder le patrimoine culturel se retrouve également dans des instruments tels que la Convention sur la protection du patrimoine culturel subaquatique. Au niveau régional, la Convention européenne sur les infractions visant des biens culturels a été ouverte à la signature en 1985, mais n'est pas encore entrée en vigueur.

46. L'un des instruments à caractère non contraignant qui présente un intérêt dans un contexte de droit pénal est le Traité type pour la prévention des infractions visant les biens meubles qui font partie du patrimoine culturel des peuples[43]. Certaines de ses dispositions peuvent servir de base à des dispositions normatives réprimant le trafic de biens culturels. Dans sa résolution 2003/29, le Conseil économique et social a invité les États Membres à envisager, lorsqu'il y a lieu et conformément au droit interne, d'adopter ce traité lorsqu'ils concluent des accords de ce type avec d'autres États[44].

47. Aujourd'hui, l'omniprésence et la complexité du trafic de biens culturels sont de plus en plus admises aux niveaux tant international que national. On estime que ce trafic et les infractions connexes forment un pan sans cesse croissant et de plus en plus attrayant de l'activité des organisations criminelles nationales et transnationales. Ces facteurs ont conduit les États Membres à négocier et à adopter un autre instrument à caractère non contraignant que sont les Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes, cadre qui peut les aider à élaborer et à renforcer leurs politiques de justice pénale, leurs stratégies, leur législation et leurs mécanismes de coopération aux fins de la protection contre le trafic de biens culturels et autres infractions connexes.

48. Depuis 2000, les organismes intergouvernementaux expriment leur inquiétude croissante au sujet du trafic de biens culturels. Lorsqu'elle a adopté la Convention des Nations Unies contre la criminalité transnationale organisée, l'Assemblée générale s'est déclarée, dans le préambule de sa résolution 55/25, fermement convaincue que la Convention constituerait un outil efficace et le cadre juridique nécessaire de la coopération internationale dans la lutte contre, notamment, les atteintes au patrimoine culturel[45].

---

[43] *Huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, La Havane, 27 août-7 septembre 1990: rapport établi par le Secrétariat* (publication des Nations Unies, numéro de vente: F.91.IV.2), chap. I, sect. B.1, annexe.

[44] Voir également le Principe 14 des Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes. Il convient également de noter que l'Assemblée générale, dans sa résolution 68/186, a prié l'ONUDC de continuer d'examiner le Traité type en tenant compte des vues et observations exprimées par les États Membres, demandant à ces derniers et aux organisations internationales compétentes qui ne l'avaient pas encore fait de soumettre au Secrétariat leurs commentaires sur le Traité.

[45] Le document CTOC/COP/2010/12 contient une analyse des éléments qui intéressent l'applicabilité de la Convention dans ce domaine.

49. Par la suite, le Conseil économique et social a exprimé, dans ses résolutions 2004/34 et 2008/23, son inquiétude quant à l'implication de groupes criminels organisés dans le trafic de biens culturels volés, affirmant la nécessité de mettre en place une coopération internationale pour combattre ce trafic. Dans sa résolution 2010/19, le Conseil a estimé qu'il faudrait pleinement utiliser la Convention contre la criminalité organisée et la Convention des Nations Unies contre la corruption pour renforcer la lutte contre le trafic de biens culturels, y compris, au besoin, en étudiant d'autres moyens normatifs possibles. À sa cinquième session, en 2010, la Conférence des Parties à la Convention contre la criminalité organisée a adopté la résolution 5/7, dans laquelle elle a exhorté les États parties à se servir de la Convention comme support d'une large coopération visant à prévenir et à réprimer les infractions pénales visant des biens culturels, en particulier à restituer le produit du crime ou les biens à leurs propriétaires légitimes, conformément à l'article 14, paragraphe 2, de la Convention. En outre, l'Assemblée générale a invité, dans ses résolutions 66/180 et 68/186, les États Membres à envisager, au besoin, de revoir leurs cadres juridiques afin de pouvoir offrir la coopération internationale la plus large possible pour s'attaquer véritablement au problème du trafic de biens culturels, les invitant également à ériger le trafic de biens culturels, y compris le vol et le pillage sur des sites archéologiques et d'autres sites culturels, en infraction grave, au sens de l'article 2 de la Convention des Nations Unies contre la criminalité transnationale organisée, en vue d'utiliser pleinement cette Convention aux fins d'une large coopération internationale dans la lutte contre toutes les formes et tous les aspects du trafic de biens culturels et les infractions connexes. En application de ces résolutions, les États Membres ont élaboré les Principes directeurs internationaux mentionnés plus haut.

50. Les Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes contiennent des chapitres sur les sujets suivants: a) stratégies de prévention du crime (collecte d'informations et de données, rôle des institutions culturelles et du secteur privé, surveillance du marché des biens culturels, importations et exportations et sites archéologiques, et éducation et sensibilisation du public); b) politiques de justice pénale (respect et application des traités internationaux pertinents, incrimination de certains comportements préjudiciables ou création d'infractions administratives, responsabilité des entreprises, saisie et confiscation, enquêtes); c) coopération internationale (juridiction, extradition, saisie et confiscation, coopération entre services de poursuite et d'enquête, et retour, restitution ou rapatriement de biens culturels); et d) application des Principes à toute situation, y compris des circonstances exceptionnelles, qui favorise le trafic de biens culturels et les infractions connexes.

51. La réponse au trafic de biens culturels dépend largement de la coopération et de la coordination entre États et de la création de partenariats public-privé. Cette coopération et ces partenariats peuvent consister, par exemple, à entrer des informations complètes dans les inventaires et les bases de données, qui peuvent être des outils importants pour déterminer la provenance d'un objet culturel avant qu'il ne soit vendu sur le marché légitime, y compris dans des maisons d'enchères, et faciliter l'investigation d'un vol et d'un trafic potentiel. Outre les inventaires et bases de données des pays, la base de données d'INTERPOL sur les œuvres d'art

volées[46] combine la description précise et des images d'environ 43 000 objets, ce qui peut être particulièrement utile dans les affaires transnationales. Les 13 "listes rouges"[47] déjà émises par le Conseil international des musées, organisation non gouvernementale internationale, classent les objets archéologiques ou œuvres d'art menacés dans les régions les plus exposées du monde, comme l'Afghanistan, Haïti et la République arabe syrienne, afin d'empêcher qu'ils ne soient vendus ou exportés illégalement. L'Art Loss Register[48] est une grande base de données privée qui répertorie les œuvres d'art, antiquités et objets de collection perdus ou volés. Elle contient également des détails d'œuvres qui n'ont pas été volées, ce qui peut dissuader des voleurs potentiels et aider à récupérer les œuvres[49] en cas de vol.

52. L'importance d'une réponse coordonnée est encore illustrée par l'initiative de sensibilisation qu'ont lancée conjointement l'ONUDC, l'Organisation mondiale du tourisme et l'UNESCO, qui invite les voyageurs à aider à combattre plusieurs formes de trafic, dont celui de biens culturels[50]. Un autre exemple utile de coopération importante entre les organisations intergouvernementales, les organismes nationaux et le secteur privé est la création, par le Conseil international des musées, de l'Observatoire international du trafic illicite des biens culturels[51], plate-forme collaborative qui fournit des informations et des moyens aux personnes et organisations concernées.

IV. Conclusions et recommandations

53. Bien que la cybercriminalité et le trafic puissent différer en termes d'objet principal de l'infraction, il apparaît clairement que de nouveaux facteurs, y compris la mondialisation et l'avènement de nouvelles technologies, forment, dans chaque domaine, le terreau sur lequel de nouveaux marchés illicites prennent racine. À mesure que ces racines et facteurs se développent, il en va de même du risque que ces deux types de criminalité s'étendent et causent des pertes et des dommages croissants. En ce qui concerne la cybercriminalité, notamment, le marché potentiel, qu'il s'agisse d'extorsion en ligne, de vente illicite en ligne ou de violation et de vente de données, est en pleine expansion car de plus en plus de gens, dans le monde, utilisent l'Internet. Il est donc essentiel, si l'on veut apporter des réponses efficaces, d'anticiper et de se préparer à l'évolution future des marchés illicites de la cybercriminalité et du trafic de biens culturels.

---

[46] www.interpol.int/Crime-areas/Works-of-art/Database.

[47] http://icom.museum/programmes/fighting-illicit-traffic/red-list.

[48] www.artloss.com/en.

[49] Il convient de noter que l'article 5 b) de la Convention concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels exige des États parties qu'ils établissent et tiennent à jour, sur la base d'un inventaire national de protection, la liste des biens culturels importants, publics et privés, dont l'exportation constituerait un appauvrissement sensible du patrimoine culturel national. À titre préventif, le Principe 1 des Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes énonce que "Les États devraient envisager de constituer et de développer des inventaires ou des bases de données, le cas échéant, de biens culturels aux fins de la protection contre leur trafic. L'absence d'enregistrement dans lesdits inventaires n'exclut en aucun cas les biens culturels de la protection".

[50] Pour de plus amples informations: www.bearesponsibletraveller.org.

[51] http://obs-traffic.museum.

54. Il faut, pour commencer, effectuer une recherche systématique et obtenir des statistiques à jour, fiables et accessibles sur les deux types de criminalité. Comme le note le rapport du Groupe consultatif d'experts indépendants sur la révolution des données pour le développement durable[52], il faut trouver un "consensus mondial sur les données" dans lequel la technologie et l'innovation puissent être partagées et utilisées pour le bien commun, y compris à travers un réseau mondial d'innovation en matière de données. Cela s'applique également à la façon dont nous comprenons et mesurons les nouveaux défis que présentent, dans le monde, des activités criminelles telles que la cybercriminalité et le trafic de biens culturels.

55. Pour combattre la cybercriminalité et le trafic de biens culturels, on pourrait notamment prendre les mesures suivantes:

a) Les États Membres pourraient envisager de renforcer leur capacité à tenir des registres des infractions et d'échanger, aux niveaux régional et international, des informations sur l'implication de groupes criminels organisés, le mode opératoire de ces groupes et les techniques utilisées pour déterminer les formes de cybercriminalité et de trafic de biens culturels;

b) Il faudrait faciliter l'interaction entre les entreprises privées, qu'il s'agisse de fournisseurs de services Internet, de banques, d'entreprises mondiales de logistique et de livraison, de musées ou de maisons d'enchères, ou les institutions publiques, qu'il s'agisse d'acteurs de l'application de la loi ou de la justice pénale, par des partenariats public-privé, propres à renforcer la confiance et le dialogue. Plus largement, des réponses réglementaires qui iraient au-delà du droit pénal et encourageraient la participation active du secteur privé à la prévention de la criminalité pourraient être utiles pour créer un environnement sensible aux nouvelles menaces et pour détecter et combattre ces dernières;

c) Les États Membres pourraient envisager de revoir et de renforcer leurs cadres nationaux destinés à prévenir et à combattre le trafic de biens culturels, notamment lorsque ces biens sont particulièrement exposés au trafic, par exemple en utilisant les Principes directeurs internationaux sur les mesures de prévention du crime et de justice pénale relatives au trafic de biens culturels et autres infractions connexes. Dans le domaine de la cybercriminalité, ils pourraient envisager d'adopter une démarche juridique équilibrée qui utiliserait les infractions spécifiques pour incriminer des actes commis contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques, tout en étudiant l'applicabilité d'autres infractions générales, comme le vol, la fraude, la contrefaçon et le préjudice personnel, à des actes commis en ligne;

d) Il se pourrait que les États Membres aient besoin d'étudier les moyens de promouvoir la coopération internationale en matière pénale. Dans le domaine de la cybercriminalité, cela pourrait nécessiter, en particulier, d'étudier les possibilités d'accélérer les procédures officielles d'entraide judiciaire et de renforcer la coopération en matière d'application de la loi, et de poursuivre le dialogue multilatéral en ce qui concerne l'accès transnational aux données informatiques. Dans le domaine du trafic de biens culturels, cela pourrait nécessiter de mettre davantage l'accent sur l'investigation et la poursuite des réseaux criminels par l'échange d'informations entre les services nationaux spécialisés;

____

[52] *A World that Counts: Mobilising the Data Revolution for Sustainable Development* (novembre 2014) (www.undatarevolution.org).

e) Il faut que la recherche et les études statistiques, les partenariats public-privé, les cadres législatifs et les mécanismes de coopération internationale soient soutenus par une capacité effective au niveau national. Il importe de mettre en place une assistance technique et une coopération si l'on veut diffuser de bonnes pratiques d'enquête, des données d'expérience et de nouvelles techniques. Dans le domaine de la cybercriminalité, les États Membres pourraient souhaiter renforcer le partage de nouvelles méthodes d'enquête sur des fraudes financières complexes commises sur Internet, le trafic de drogues en ligne ou l'utilisation de monnaies virtuelles à des fins de blanchiment d'argent, ce qui permettrait aux services de détection et de répression de plusieurs pays d'acquérir rapidement les compétences requises pour contrer les nouvelles menaces. En ce qui concerne le trafic de biens culturels, les États Membres pourraient souhaiter renforcer l'aptitude des services frontaliers et douaniers à identifier les biens culturels objets d'un trafic, examiner les relations qui existent entre les services nationaux chargés de combattre le blanchiment d'argent et le trafic de biens culturels, et recenser et échanger de bonnes pratiques dans tous les domaines de l'action menée en matière de prévention du crime et de justice pénale contre le trafic de biens culturels;

f) Il faudrait que l'ONUDC continue de proposer aux États Membres une assistance technique qui permette de renforcer l'action de prévention du crime et de justice pénale menée contre les nouvelles formes de criminalité, y compris la cybercriminalité, le trafic de biens culturels et les infractions connexes, sur demande et en coordination avec les organisations internationales compétentes. Les États Membres pourraient souhaiter envisager, à titre de priorité, de mettre des fonds à disposition à cette fin;

g) Les États Membres pourraient souhaiter adopter, contre la cybercriminalité et le trafic de biens culturels, une approche holistique qui tiendrait compte à la fois des modes opératoires et des menaces que l'on rencontre aujourd'hui et des possibles évolutions futures de la criminalité. Les réponses devront s'appuyer de plus en plus sur la coopération mondiale, la participation de multiples acteurs et le recours à la technologie, qu'il s'agisse de bases de données ou de plates-formes de communications sécurisées.