Naciones Unidas A/CONF.222/12

13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Distr. general
2 de febrero de 2015
Español
Original: inglés

Doha, 12 a 19 de abril de 2015

Tema 5 del programa provisional*
Enfoques amplios y equilibrados para prevenir y afrontar adecuadamente las formas nuevas y emergentes de delincuencia transnacional

Seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia pena frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional**

Documento de antecedentes

Resumen

En el presente documento de antecedentes se describen a grandes rasgos los aspectos comunes y específicos de las respuestas en materia de prevención del delito y justicia penal frente a la ciberdelincuencia y el tráfico de bienes culturales, dos ejemplos destacados de delincuencia en evolución que han adquirido cada vez más relevancia como consecuencia de la globalización y el desarrollo de la tecnología de la información. Si bien los grupos de delincuencia organizada han sabido aprovechar las oportunidades que ofrecen estos fenómenos, es preciso adoptar medidas eficaces para conocer mejor la escala, las raíces y el *modus operandi* en la comisión de delitos conexos, elaborar estrategias eficaces de prevención, mejorar el intercambio de información, y reforzar los marcos nacionales y la cooperación internacional entre Estados Miembros.

* A/CONF.222/1.

** La Secretaría de las Naciones Unidas desea manifestar su agradecimiento a los miembros de la red del programa de las Naciones Unidas en materia de prevención del delito y justicia penal, en especial al Instituto Nacional de Justicia del Departamento de Justicia de los Estados Unidos, al Consejo Consultivo Internacional Científico y Profesional, al Instituto Coreano de Criminología y al Instituto Europeo de Prevención del Delito y Lucha contra la Delincuencia, afiliado a las Naciones Unidas, por su ayuda en la preparación y organización del seminario.

V.15-00666 (S) 230215 230215

Índice

I. Introducción

1. En las reuniones preparatorias regionales para el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente que tuvieron lugar en Asia y el Pacífico, Asia Occidental y África, los Estados Miembros reconocieron la importancia de elaborar una respuesta integral frente a los delitos en evolución, concretamente el delito cibernético y el tráfico de bienes culturales[1]. Al igual que ocurre con muchos otros delitos, las estrategias eficaces de prevención y las medidas de justicia penal frente a estas formas de delincuencia en evolución tienen su fundamento en una base detallada de conocimientos y una clara comprensión de los elementos facilitadores del delito y de las tendencias delictivas.

2. En el documento de trabajo preparado por la Secretaría sobre enfoques amplios y equilibrados para prevenir y afrontar adecuadamente las formas nuevas y emergentes de delincuencia transnacional[2], se examina una tipología multidimensional de las formas nuevas y emergentes de delincuencia, a partir de sus posibles raíces y elementos impulsores, así como de su *modus operandi* comunes. La globalización; la proximidad de la pobreza, los conflictos y la fragilidad del estado de derecho frente a mercados de alto valor; así como la rápida aparición de nuevas formas de tecnología moderna se señalaron como posibles raíces y elementos impulsores de las nuevas formas de delincuencia. En el documento se señalaron además algunos cambios en la estructura de los grupos delictivos organizados y el uso de la corrupción para facilitar la comisión de delitos como principales *modus operandi*.

3. Junto a otros tipos de delitos como la piratería, el abuso y la explotación de los niños y el tráfico de fauna y flora silvestres, los delitos del tráfico de bienes culturales y la ciberdelincuencia se incluyen habitualmente en la categoría de delitos emergentes o en evolución[3]. Como se señala en el documento A/CONF.222/8, dichos actos no tienen que ser siempre enteramente nuevos, sino que pueden suponer un resurgimiento de tipos de delitos “convencionales” o bien la evolución de nuevas formas y medios para la comisión de delitos ya tipificados.

4. El robo y el tráfico de bienes culturales a escala nacional, por ejemplo, existen desde hace siglos. Sin embargo, ha sido durante las últimas décadas que la comunidad internacional se ha esforzado por regular el comercio de bienes culturales y tipificar específicamente como delito el robo de obras de arte y antigüedades. Al mismo tiempo, la globalización ha facilitado la creciente participación de grupos delictivos organizados en estas actividades, lo que ha llevado a la aparición de mercados ilícitos globalizados de bienes culturales robados y a la posibilidad de que grupos delictivos organizados y quizás también grupos terroristas obtengan importantes beneficios de ellos. Del mismo modo, desde la década de 1960 muchos países han reconocido como delitos ciertos actos relacionados con la informática, como el uso no autorizado de sistemas informáticos y la manipulación de datos electrónicos. Pero ha sido con la llegada de Internet que

---

[1] A/CONF.222/RPM.1/1, párrs. 33 y 35; A/CONF.222/RPM.2/1, párrs. 38 y 40; y A/CONF.222/RPM.4/1, párr. 70.

[2] A/CONF.222/8.

[3] Véase, por ejemplo, la resolución 66/181 de la Asamblea General, párr. 18.

las tecnologías globalizadas de la información y las comunicaciones han empezado a usarse para cometer delitos a escala internacional, en la forma de ciberdelincuencia que conocemos actualmente.

5. En este sentido, tanto la ciberdelincuencia como el tráfico de bienes culturales son buenos ejemplos del impacto que pueden tener las raíces y elementos impulsores, como la globalización y la aparición de nuevas formas de tecnología sobre la innovación en el ámbito de la delincuencia. Si bien los dos tipos de delitos difieren en varios aspectos, como por ejemplo su objeto primario, también tienen muchos otros elementos en común.

6. El tráfico de bienes culturales está relacionado con el robo, el tráfico y la venta de objetos tangibles que poseen valor en razón de su especial relevancia para el patrimonio cultural. Si bien el objeto de la ciberdelincuencia a menudo es intangible, como por ejemplo los datos o sistemas informáticos, una parte de los delitos informáticos se centran en el robo y la reventa. Los actos relacionados con la informática que se realizan en provecho propio, para obtener beneficios económicos o para perjudicar económicamente a otros, pueden consistir, por ejemplo, en el robo por Internet de datos de cuentas bancarias o tarjetas de crédito y su reventa orientada al fraude financiero o al robo. Al igual que ocurre en el tráfico de bienes culturales, el vendedor y el comprador pueden hallarse en jurisdicciones distintas.

7. Por lo que respecta al nivel de organización delictiva, los grupos implicados en la ciberdelincuencia pueden mostrar una estructura relativamente fluida[4]. No obstante, cada vez hay más pruebas de que los grupos de estructura jerárquica tradicional utilizan un modelo basado en servicios característico del mercado de la ciberdelincuencia con el fin de llevar a cabo delitos más complejos[5]. En este sentido, puede haber una intersección entre las esferas del tráfico de bienes culturales y de la ciberdelincuencia en el nivel de la venta ilícita de bienes culturales a través de Internet. La Organización Internacional de Policía Criminal (INTERPOL), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) y el Consejo Internacional de Museos han reconocido, por ejemplo, que el comercio ilícito de bienes culturales a través de Internet es un problema cada vez más grave, tanto para los países de origen como para los de destino[6]. En relación con este problema, las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos[7] recomiendan el establecimiento de mecanismos de denuncia y vigilancia orientados específicamente al comercio de bienes culturales a través de Internet[8].

---

[4] Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), *Comprehensive Study on Cybercrime* (2013, draft), pág. 46; y Blythe Bowman Proulx, “Organized criminal involvement in the illicit antiquities trade”, *Trends in Organized Crime*, vol. 14, núm. 1 (marzo de 2011).

[5] Oficina Europea de Policía (EUROPOL), *The Internet Organised Crime Threat Assessment 2014* (La Haya, 2014), pág. 10.

[6] UNESCO, INTERPOL y Consejo Internacional de Museos, “Basic Actions concerning Cultural Objects being offered for Sale over the Internet”. Disponible en www.unesco.org/new/en/culture/themes/illicit-trafficking-of-cultural-property.

[7] Resolución 69/196 de la Asamblea General, anexo.

[8] Directrices 3 d) y 10.

8. Además de la naturaleza de los propios delitos y de la intersección recién descrita, también existen elementos comunes en el nivel de la prevención del delito y de la reunión de información a los fines de la justicia penal. Nunca ha habido información detallada sobre estadísticas y tendencias en relación con ambos delitos. Hasta hace poco, buena parte de lo que se sabía acerca del tráfico de bienes culturales procedía de estudios monográficos sobre formas específicas del delito, como el robo de objetos de arte o el saqueo de antigüedades históricas. No obstante, se han hecho esfuerzos por ampliar la información disponible reuniendo datos relativos a estadísticas policiales y judiciales sobre tráfico ilícito, robo, posesión, manejo y excavación ilegal de bienes culturales, por ejemplo mediante el Estudio de las Naciones Unidas sobre Tendencias Delictivas y Funcionamiento de los Sistemas de Justicia Penal. Los resultados obtenidos confirman la necesidad de reunir de manera continua y sistemática datos que permitan llegar a conclusiones representativas. No obstante, el gran número de actos distintos que entran en la categoría general de "ciberdelincuencia" también plantea problemas cuando se trata de reunir datos. Con todo, las metodologías basadas en el uso de diversas fuentes de datos permiten adoptar enfoques prometedores en este sentido.

9. Si bien la comisión del delito puede producirse [en ambos casos] dentro de una única jurisdicción, el tráfico de bienes culturales y la ciberdelincuencia también tienen en común el elemento de la transnacionalidad, lo que hace que la cooperación internacional sea un factor esencial en la búsqueda de respuestas eficaces. A ese respecto, en todas las reuniones preparatorias regionales para el 13º Congreso[9] se subrayó la importancia fundamental de promover la cooperación internacional. En relación con la ciberdelincuencia, se calcula que entre el 30 y el 70% de los delitos cibernéticos tienen una dimensión transnacional[10]. El tráfico de bienes culturales, por su parte, es un delito principalmente transnacional[11]. La investigación de los delitos que afectan a múltiples jurisdicciones requiere la asistencia judicial recíproca más amplia posible con respecto a las investigaciones, los procesos y las actuaciones judiciales, a fin de aumentar la eficacia de los procedimientos y agilizarlos.

10. La cooperación internacional se ve facilitada cuando en los marcos jurídicos nacionales se tipifican como delito las mismas conductas sustantivas subyacentes. En el caso del tráfico de bienes culturales, los delitos específicos pueden incluir el tráfico, la exportación y la importación ilícitas, y el robo de bienes culturales, así como el saqueo y la excavación ilícita de emplazamientos arqueológicos y culturales[12]. En el caso de la ciberdelincuencia, se requieren habitualmente disposiciones penales específicas para tipificar como delito conductas dirigidas contra datos o sistemas informáticos, como por ejemplo el delito de acceso ilegal a un sistema o a datos informáticos.

11. Por último, la eficacia de las respuestas ante ambos tipos de delito probablemente sea mayor cuando el enfoque adoptado esté coordinado entre los diversos interesados. Buena parte de la infraestructura de Internet, de la que

---

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

[10] UNODC, *Comprehensive Study on Cybercrime*, pág. 183.

[11] CTOC/COP/2010/12, párr. 33.

[12] Véase la directriz 16 de las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos.

dependen muchas formas de ciberdelincuencia y de tráfico de bienes culturales, es de propiedad y gestión privada. Los objetos de valor cultural pueden hallarse bajo diversas formas de propiedad, ya sea del Estado, de particulares, de museos, de fideicomisos o de otras asociaciones no gubernamentales. La participación de todas las partes interesadas pertinentes, por ejemplo mediante alianzas público-privadas, es fundamental para la sensibilización acerca del riesgo que suponen esos delitos y para promover buenas prácticas preventivas, así como para facilitar las investigaciones y disponer medidas de indemnización o reparación para las víctimas.

12. Este documento de antecedentes pretende desarrollar el marco establecido en el documento A/CONF.222/8, con el fin de ilustrar las lecciones aprendidas y las estrategias de cooperación internacional frente a los tipos de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales. El documento examina la base de conocimientos disponibles para cada tipo de delito, evalúa los problemas y la práctica desarrollada a partir de los enfoques legislativos nacionales, las modalidades de investigación y las formas de cooperación internacional. Si procede, se señalan los ámbitos en que pueden adoptarse medidas de prevención del delito. También analiza las acciones que pueden emprender tanto los Estados como la comunidad internacional en su conjunto para fortalecer las respuestas de prevención del delito y justicia penal a nivel mundial.

II. Ciberdelincuencia

A. Definición del problema

13. En 1994, en el *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos* se señaló que el potencial de la delincuencia informática es tan amplio como el de los propios sistemas internacionales de telecomunicaciones[13]. Como era de esperar, la palabra “Internet” aparecía solo una vez en el Manual y la palabra “ciberdelincuencia” no se utilizó; sin embargo, las conclusiones demostraron una gran visión de futuro. Si bien el Manual centró su atención en el concepto de “delito informático”, es bien sabido que hoy en día la “ciberdelincuencia” recurre efectivamente a las tecnologías globalizadas de la información y las comunicaciones, en particular a Internet, para la comisión de actos delictivos de alcance transnacional.

14. Con la evolución de la terminología, se han realizado esfuerzos para formular una definición académica del término “ciberdelincuencia”[14]. Un enfoque moderno de la cuestión consiste en reconocer que la ciberdelincuencia no es necesariamente un término jurídico técnico, sino más bien un término genérico para referirse a un conjunto de hechos cometidos en contra o a través del uso de datos o sistemas

---

[13] Naciones Unidas, *Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos*, Revista Internacional de Política Criminal, Serie M, Núms. 43 y 44 (publicación de las Naciones Unidas, núm. de venta S.94.IV.5), párr. 12.

[14] Véase, por ejemplo, David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, Polity Press, 2007).

informáticos. Otros enfoques se centran en los delitos contra la información computadorizada o el uso de recursos de información con fines ilícitos[15].

15. Los actos comprendidos habitualmente en la categoría de "ciberdelincuencia" son aquellos en los que los datos o sistemas informáticos son el objeto contra el que se dirige el delito, así como los actos en que los sistemas informáticos o de información forman parte integrante del *modus operandi* del delito. Algunos ejemplos de los primeros son los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos, como el acceso ilegal a datos o sistemas informáticos (a veces denominados delitos cibernéticos "principales"). Algunos ejemplos de los segundos son el uso de datos o sistemas informáticos para estafar, robar o causar daño a otras personas, así como los delitos relacionados con contenidos informáticos o de Internet, como los discursos de incitación al odio, la pornografía infantil, los delitos relacionados con la identidad y la venta por Internet de mercancías ilícitas[16].

16. Sin embargo, en términos generales, la frontera entre la "ciberdelincuencia" y la "delincuencia convencional" resulta cada vez más difusa. Con el uso cada vez más generalizado de dispositivos electrónicos y de la conectividad global en la vida cotidiana, las pruebas electrónicas, como los mensajes de texto, los mensajes electrónicos, los datos de navegación por Internet o los datos de redes sociales, son cada vez más habituales en muchas investigaciones penales convencionales. Los instrumentos forenses digitales y los requerimientos a proveedores de servicios electrónicos a que se recurre en estos casos, así como muchos de los problemas y buenas prácticas de investigación, son a menudo los mismos que en los casos de ciberdelincuencia. En ese sentido, si bien este documento de antecedentes se centra en actos que habitualmente se consideran casos de ciberdelincuencia, muchas de sus observaciones y conclusiones se aplican de manera más amplia a las pruebas electrónicas en general.

17. Uno de los principales elementos impulsores de la ciberdelincuencia contemporánea y del uso creciente de pruebas digitales es el desarrollo de la conectividad electrónica global. Hoy existen casi 3.000 millones de usuarios de Internet, cerca del 40% de la población mundial. El acceso mayoritario a Internet es por medio de banda ancha móvil, que llega aproximadamente al 32% de la población mundial, casi cuatro veces la cifra de 2009[17]. Se prevé que en 2018 el número de dispositivos conectados a redes de protocolo Internet ("IP") alcanzará prácticamente el doble de la población mundial[18].

18. El rápido crecimiento de Internet y de la tecnología informática ha facilitado el crecimiento económico y un mayor acceso a servicios esenciales como la educación, la atención de salud y la gobernanza electrónica, pero también ha creado nuevas posibilidades para la actividad delictiva. Algunos instrumentos de ciberdelincuencia como las redes robot o zombi ("botnets" -término derivado de las palabras "robot"

---

[15] Véase, por ejemplo, el Acuerdo sobre la Cooperación entre los países de la CEI para luchar contra el delito en la esfera de la información computadorizada (2001).

[16] UNODC, *Comprehensive Study on Cybercrime*, pág.16.

[17] Unión Internacional de Telecomunicaciones, "The World in 2014: ICT facts and figures" (Ginebra, 2014).

[18] Cisco, "The zettabyte era: trends and analysis", Cisco Visual Networking Index (San Jose, California, 2014).

y “network”), pueden constituir redes globales de decenas o centenares de miles de dispositivos infectados con programas informáticos maliciosos controlados a distancia por delincuentes. Las páginas web de los medios sociales pueden utilizarse para cometer actos de hostigamiento, incitación al odio, amenazas de violencia, extorsión, o para la difusión de información privada a escala global en cuestión de segundos. Como los delincuentes intentan también extender sus actividades a la “Internet de los objetos”, también existe la posibilidad de que las actividades delictivas a escala mundial aumenten aún más.

19. Además del carácter global del problema, en los últimos diez años se han experimentado ciclos en el nivel de anonimato que ofrece Internet, lo que ha dado lugar a su utilización para la comisión de actos delictivos. En los primeros tiempos se daba por sentado que Internet era en gran medida un medio anónimo, por lo menos a juicio de sus usuarios, que no comprendían que era posible técnicamente rastrear la actividad en línea de una persona. Sin embargo, en los últimos años los sistemas de justicia penal se han venido familiarizando más con los conceptos de direcciones IP y registros de conexión, así como con el uso de órdenes judiciales para obtener datos de proveedores de servicios electrónicos. Como resultado de ello, las huellas electrónicas que dejan los usuarios de Internet resultan cada vez más accesibles para los investigadores, aunque la obtención de datos de Internet puede requerir mucho tiempo y esfuerzo. Asimismo, los avances con respecto a los instrumentos forenses digitales, como la creación de dispositivos forenses de instalación automática (“plug and play”) y sencillos de utilizar, han facilitado el análisis rutinario de los datos almacenados en dispositivos digitales como computadoras y teléfonos inteligentes.

20. La tecnología no deja de progresar, y los instrumentos forenses y las técnicas actuales de investigación de la ciberdelincuencia afrontan retos inimaginables hace apenas una década. Por ejemplo, la existencia de software gratuito y de fácil acceso que permite la encriptación de 256 bits de archivos o de dispositivos enteros de almacenamiento de datos. Si no se dispone de contraseña o de clave, los datos encriptados de esa manera resultan prácticamente inaccesibles para las autoridades encargadas de hacer cumplir la ley. Las encriptaciones más avanzadas, de 2.048 bits, resultan teóricamente indescifrables en la actualidad. Las nuevas redes descentralizadas y anonimizadoras, a menudo conocidas como la “Internet profunda”, funcionan junto con la Internet convencional. Algunos servicios como Onion Router (“Tor”) hacen que resulte muy difícil para las autoridades encargadas de hacer cumplir la ley determinar el origen de las comunicaciones electrónicas o la identidad de las páginas web de “servicios ocultos”. Esos “servicios ocultos” pueden usarse para albergar anónimamente mercados ilícitos de drogas, armas o pornografía infantil. Algunas de esas redes ofrecen también la posibilidad de almacenar datos de forma descentralizada y encriptada entre los distintos “nodos” participantes. Los documentos o imágenes electrónicos así almacenados son también prácticamente inaccesibles para las autoridades encargadas de hacer cumplir la ley. Las implicaciones de esas tecnologías son profundas y plantean la cuestión de cómo lograr que las respuestas de las autoridades se mantengan a la par con el ritmo de innovación de la ciberdelincuencia.

B. Medición de la ciberdelincuencia

21. Uno de los enfoques utilizados para medir las nuevas formas y dimensiones de la delincuencia, incluida la ciberdelincuencia, se basa en una combinación de indicadores, como por ejemplo información sobre los infractores; información sobre los flujos existentes en los mercados ilícitos; e información sobre el número de delitos cometidos, los daños y pérdidas causados, y los flujos financieros ilícitos resultantes. En el caso de la ciberdelincuencia se pueden utilizar diversas fuentes de datos con ese fin. Algunas de ellas son las estadísticas de delitos registrados por la policía; las encuestas entre particulares y empresas; las iniciativas de denuncia de las víctimas; y la información de ciberseguridad obtenida por medios tecnológicos. Otras fuentes incluyen técnicas como el rastreo de URL o el secuestro de redes zombi o "botnets".

22. Si bien debe prestarse atención a las estadísticas de los delitos cibernéticos registrados por la policía no cabe duda de que tienen importantes limitaciones, pues en la mayoría de los casos las víctimas no presentan denuncias. En una encuesta realizada entre 20.000 usuarios de Internet de 24 países, solo el 21% de los encuestados que afirmaron haber sido víctimas de delitos cibernéticos habían denunciado el hecho ante la policía[19]. A nivel mundial, las autoridades encargadas de hacer cumplir la ley a veces utilizan metodologías y enfoques estadísticos distintos, lo que dificulta las comparaciones internacionales. Además, el volumen total de los delitos cibernéticos registrados por la policía está estrechamente relacionado con el número de policías especializados, lo que sugiere que las estadísticas podrían reflejar la actividad investigadora de la policía más que el número de víctimas de los delitos cibernéticos[20].

23. Las encuestas sobre las víctimas de esos delitos realizadas entre particulares y empresas constituyen una importante fuente alternativa de información. Según las encuestas, en el caso de la población general, el número de víctimas de delitos cibernéticos es considerablemente superior al correspondiente a delitos "convencionales". El porcentaje de víctimas de fraude en línea con tarjetas de crédito, robo de identidad, respuestas a un intento de suplantación de identidad o "phishing", o acceso no autorizado a un correo electrónico, varía entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, mientras que el porcentaje de delitos típicos, como el robo, el hurto y el robo de coches en esos mismos países es inferior al 5%[21]. Las empresas del sector privado también comunican porcentajes similares respecto de las víctimas. En Europa, por ejemplo, el porcentaje de víctimas se sitúa entre el 2 y el 16% en el caso de delitos como la violación de datos por intrusión o "phishing"[22]. En un estudio se determinó que en 2012 las víctimas del delito de usurpación de identidad aumentaron en más de un millón de personas y que los infractores robaron más de 21.000 millones de dólares

---

[19] Symantec, "Norton Cybercrime Report", 2012. Disponible en http://us.norton.com/cybercrimereport.

[20] UNODC, *Comprehensive Study on Cybercrime*, anexo 2.

[21] Datos proporcionados por Symantec.

[22] Eurostat, Estadísticas sobre la sociedad de la información, Encuesta comunitaria sobre el uso de las TIC y el comercio electrónico en las empresas, 2011. Disponible en francés e inglés únicamente en http://ec.europa.eu/eurostat/web/information-society/data/database.

EE.UU., la cifra más elevada desde 2009, aunque considerablemente inferior a los 47.000 millones de dólares de pérdidas estimadas en 2004[23].

24. Los datos de las encuestas que incluyen información sobre pérdidas financieras derivadas de la ciberdelincuencia pueden utilizarse para hacer estimaciones sobre su impacto. En una de las encuestas, los consumidores de 24 países del mundo que habían sido víctimas de delitos cibernéticos informaron de pérdidas medias directas de entre 50 y 850 dólares como resultado de delitos sufridos durante un año[24]. A partir de los datos de varias encuestas, se realizó un estudio en que se estimó que los costes totales directos, indirectos y de defensa a nivel mundial de varias formas de ciberdelincuencia, incluido el fraude bancario en línea, el fraude en línea con tarjetas de crédito y el fraude en los pagos anticipados, ascendía a cientos o miles de millones de dólares al año[25].

25. El análisis de los mercados de la ciberdelincuencia también permite estimar la naturaleza y la dimensión de algunas formas de delitos cibernéticos. Un enfoque de este tipo se centra en el análisis de foros en línea que funcionan como "redes sociales" para delincuentes, que tienen por objeto la venta y la compra de bienes sociales, así como el intercambio de información sobre actividades delictivas.

26. En un estudio realizado en 2011 se utilizaron datos obtenidos de seis foros clandestinos en línea, que contenían más de 2.500.000 comentarios y 900.000 mensajes privados de más de 100.000 usuarios. Las mercancías que se intercambiaban con más frecuencia en estos foros eran las tarjetas de crédito, los datos de cuentas bancarias y los instrumentos necesarios para la comisión de fraudes[26]. Un análisis reciente de los temas de fondo de 13 foros en línea indica que en ellos se ofrecen listas de datos sobre tarjetas de crédito robadas por un precio medio de unos 100 dólares y se pueden comprar instrumentos con fines delictivos como dispositivos de captura de datos de tarjetas de crédito por un precio medio de 2.400 dólares[27]. Las nuevas tecnologías de investigación también ofrecen la posibilidad de rastrear los servicios ocultos en Tor. Estas tecnologías pueden facilitar la identificación y clasificación sistemática del número y el tipo de páginas de Internet profunda relacionadas con temas como la venta de drogas ilícitas, la pornografía infantil, la venta de armas o instrumentos para cometer delitos cibernéticos[28].

27. Por último, la caracterización de los autores de estos delitos ayuda a comprender la naturaleza y el *modus operandi* de las organizaciones delictivas en cuestión. Es probable que no exista un "perfil" estándar en este sentido. Un número relativamente reducido de programadores y piratas informáticos altamente

---

[23] Javelin Strategy and Research, "2013 Identity Fraud Report: Data Breaches becoming a treasure trove for fraudsters". Disponible en: https://www.javelinstrategy.com/brochure/276.

[24] Datos proporcionados por Symantec.

[25] Ross Anderson y otros, "Measuring the cost of cybercrime", en *The Economics of Information Security and Privacy*, Rainer Böhme, ed. (Springer Berlin Heidelberg, Berlín, 2013).

[26] Marti Motoyama y otros, "An analysis of underground forums", en *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (Nueva York, ACM, 2011).

[27] Thomas Holt y Olga Smirnova, "Examining the structure, organization, and processes of the international market for stolen data", artículo de investigación elaborado para el National Institute of Justice, Rockville, Maryland, Estados Unidos de América, marzo 2014.

[28] Martijn Spitters y otros, "Towards a comprehensive insight into the thematic organization of the ToR hidden services", artículo presentado ante la IEEE Joint Intelligence and Security Informatics Conference, La Haya, septiembre de 2014.

cualificados pueden impulsar la innovación en el terreno de la ciberdelincuencia y ofrecer sus aptitudes como un servicio delictivo. Sin embargo, la facilidad de acceso a los *exploits* y los programas maliciosos implica que en muchos casos los autores ya no requieren conocimientos avanzados. Por otra parte, es posible que algunas formas de ciberdelincuencia dependan cada vez más de la presencia de un gran número de "soldados rasos". En una reciente trama de estafa con tarjetas de débito prepagadas, un grupo delictivo organizado reclutó a centenares de personas de 26 países, gracias a lo cual pudo realizar más de 40.000 retiros simultáneos de efectivo en cajeros automáticos en dos ocasiones. Se calcula que el robo fue de 45 millones de dólares[29]. Si bien más del 80 por ciento de los delitos cibernéticos tienen su origen en la delincuencia organizada[30], no cabe duda de que la variada tipología de la estructura de esos grupos, incluidas las asociaciones delictivas poco estructuradas, dificulta toda caracterización sencilla de los autores de los delitos cibernéticos.

C. Formas de prevenir y afrontar la ciberdelincuencia

28. La información sobre la naturaleza y el alcance de la ciberdelincuencia es un elemento importante que debe tenerse en cuenta al diseñar estrategias eficaces de prevención e investigación. Las estrategias de sensibilización orientadas a proteger a los consumidores contra el fraude en línea, por ejemplo, pueden requerir un enfoque distinto al de las estrategias de sensibilización en el ámbito de la protección de los niños en Internet. A este respecto, en las reuniones preparatorias regionales de Asia y el Pacífico, Asia occidental y África para el 13º Congreso, se recomendó la elaboración de instrumentos y programas que facilitaran la prevención de la ciberdelincuencia y la sensibilización al respecto. La información sobre las amenazas y las tendencias relacionadas con la ciberdelincuencia puede orientar también las respuestas en el ámbito de la investigación. La investigación de la venta de drogas ilícitas por Internet, por ejemplo, requiere competencias y técnicas distintas de las que requiere el examen forense de dispositivos informáticos. Si bien los datos disponibles sobre ciberdelincuencia pueden ayudar a centrar los esfuerzos en respuesta a las nuevas tendencias, la gran variedad de posibles delitos cibernéticos exige que los países desarrollen su capacidad en una amplia gama de respuestas en los ámbitos de la prevención y la investigación.

29. Además de la capacidad de medir la ciberdelincuencia, también deben adoptarse respuestas nacionales a la ciberdelincuencia de carácter legislativo y normativo, en ámbitos como la tipificación de delitos y las competencias procesales; la capacidad de las autoridades encargadas de hacer cumplir la ley y de la justicia penal para investigar la ciberdelincuencia, las técnicas forenses digitales y el manejo de pruebas electrónicas; los mecanismos judiciales de cooperación internacional en asuntos penales; y la prevención de la ciberdelincuencia.

---

[29] INTERPOL, "Criminal network involved in payment card fraud dismantled with INTERPOL support", 30 de abril de 2014. Disponible en http://www.interpol.int/News-and-media/News/2014/N2014-074.

[30] BAE Systems Detica y John Grieve Centre for Policing and Community Safety, *Organised Crime in the Digital Age* (London Metropolitan University, 2012).

30. Las políticas, estrategias y leyes nacionales relativas a la ciberdelincuencia son un punto de partida importante para establecer el marco general y las prioridades de las respuestas a ese delito. El archivo de datos en línea sobre ciberdelincuencia de la UNODC (que entrará en funcionamiento en 2015) contendrá detalles acerca de las estrategias nacionales de unos 50 países, y abarcará ámbitos como la sensibilización acerca de la ciberdelincuencia, la cooperación internacional, la capacidad de aplicación de la ley, la legislación, la prevención y las alianzas público-privadas. La legislación nacional sobre ciberdelincuencia también se extiende muchas veces a ámbitos como la tipificación de delitos, las facultades de investigación, la jurisdicción, las pruebas electrónicas y la cooperación internacional. El examen de las leyes nacionales sobre ciberdelincuencia muestra que los países recurren a menudo a una combinación de delitos específicos y generales para tipificar ese tipo de actos delictivos. Los delitos cibernéticos "principales", como el acceso ilícito a datos y sistemas informáticos, se tipifican a veces mediante una disposición legal específica, mientras que los delitos informáticos cometidos en provecho propio, o para obtener beneficios económicos o perjudicar económicamente a otros se tipifican más habitualmente mediante tipos delictivos generales (no relacionados específicamente con la informática)[31].

31. En algunos casos, los marcos jurídicos nacionales se promulgan en cumplimiento de instrumentos multilaterales, sean o no vinculantes, o se inspiran en ellos. Algunos de esos instrumentos son la convención relativa a la seguridad cibernética y la protección de datos personales de la Unión Africana; el acuerdo de cooperación en la lucha contra los delitos informáticos de la Comunidad de Estados Independientes; el Convenio sobre la Ciberdelincuencia del Consejo de Europa; la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, relativa a los ataques contra los sistemas de información; la convención relativa a la lucha contra los delitos informáticos de la Liga de los Estados Árabes; y el acuerdo de cooperación en el ámbito de la seguridad de la información de la Organización de Cooperación de Shanghai. En lo que respecta al posible desarrollo futuro de estos marcos multilaterales, la reunión preparatoria regional de África recomendó a los Estados que estudiaran la posibilidad de elaborar una convención sobre la ciberdelincuencia en el marco del 13º Congreso.

32. Además de disposiciones relativas a la tipificación de delitos y a las competencias procesales, los instrumentos existentes también pueden contener mecanismos de cooperación internacional para la investigación y la persecución transfronteriza de la ciberdelincuencia. Este es un ámbito que plantea cada vez más dificultades a las autoridades encargadas de hacer cumplir la ley. La llegada de la computación en la nube y del intercambio y almacenamiento de datos entre pares significa que, aun cuando en teoría sea posible localizar unos datos informáticos concretos en un momento determinado, dichos datos pueden existir en múltiples copias, pueden ser distribuidos entre múltiples dispositivos y lugares, y pueden ser trasladados a otra localización geográfica en cuestión de segundos.

33. Algunos proveedores de servicios de almacenamiento de datos, como los proveedores de servicios electrónicos o de computación en la nube del sector privado, pueden estar obligados por ley a conservar copias de los datos durante cierto tiempo, y por regla general entregarán los datos a las autoridades

[31] UNODC, *Comprehensive Study on Cybercrime*, pág. 78.

responsables de la aplicación de la ley en cumplimiento de una orden judicial o de otro proceso legal establecido a tal efecto. No obstante, cuando el proveedor o los datos se encuentran fuera de la jurisdicción encargada de la investigación, dicho proceso legal implica a menudo el uso de procedimientos oficiales y lentos de asistencia judicial recíproca entre Estados. En lo que respecta a otras formas de almacenamiento de datos, como las redes informáticas entre pares integradas por particulares, los datos pueden resultar difíciles de identificar y a menudo se encuentran almacenados de manera encriptada. En esos casos podrían requerirse medidas coercitivas para inmovilizar y entregar los datos.

34. El debate internacional acerca del actual paradigma, altamente territorializado, de las investigaciones transnacionales en materia de ciberdelincuencia y acceso a los datos sigue vivo a varios niveles[32]. Algunos de los instrumentos multilaterales existentes establecen mecanismos dirigidos a facilitar el acceso a los datos a las autoridades encargadas de hacer cumplir la ley, como el establecimiento de puntos de contacto localizables de manera ininterrumpida para las investigaciones relacionadas con la ciberdelincuencia, la conservación rápida de datos, el acceso transfronterizo a datos informáticos almacenados, con consentimiento o cuando sean de acceso público, y las solicitudes urgentes de asistencia mutua. En la práctica, no cabe duda de que, incluso con estos mecanismos, muchas autoridades encargadas de hacer cumplir la ley tienen graves problemas para conseguir un acceso rápido a datos extraterritoriales en el curso de investigaciones sobre delitos cibernéticos. Al mismo tiempo, los derechos humanos, el estado de derecho y la privacidad deben contar con salvaguardias suficientes que garanticen que el acceso de las autoridades encargadas de hacer cumplir la ley a los datos es limitado, predecible, proporcionado y se halla sometido a supervisión adecuada.

35. Innovaciones como la inclusión de un módulo de pruebas digitales en la nueva versión del Programa para Redactar Solicitudes de Asistencia Judicial Recíproca de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) pueden contribuir a agilizar los procedimientos de asistencia judicial recíproca relacionados con pruebas electrónicas. Paralelamente, no obstante, las autoridades encargadas de hacer cumplir la ley deberán ser cada vez más innovadoras en el desarrollo de formas de colaboración en las investigaciones transnacionales de delitos cibernéticos. La implicación de entidades como el Complejo Mundial para la Innovación de la INTERPOL y el Centro Europeo contra la Delincuencia Informática (EC3) de la Oficina Europea de Policía (Europol) en tareas de coordinación y apoyo de las investigaciones transnacionales, por ejemplo, facilitando el intercambio de información entre fuerzas del orden de distintas nacionalidades, podría resultar especialmente importante. Otros foros e iniciativas, como las conferencias mundiales sobre el ciberespacio, también han ofrecido a los países la oportunidad de considerar respuestas innovadoras en el ámbito de la cooperación internacional contra la ciberdelincuencia.

---

[32] Véase, por ejemplo, Consejo de Europa, “Cybercrime Convention Committee assessment report: the mutual legal assistance provisions of the Budapest Convention on Cybercrime”, documento T-CY(2013)17rev, y “Transborder access to data and jurisdiction: options for further action by the Cybercrime Convention Committee”, documento T-CY(2014)16, y Albert Rees, “International cooperation in cybercrime investigations”, ponencia preparada para el taller regional sobre delito cibernético de la Organización de los Estados Americanos, abril de 2007.

36. Las alianzas para prevenir y combatir la ciberdelincuencia, ya sea a nivel nacional o multilateral, deben incluir también al sector privado. Los proveedores de servicios de hospedaje y otros servicios en Internet pueden desempeñar un papel crucial en la prevención de la ciberdelincuencia. Pueden conservar registros útiles para la investigación de actividades delictivas, ayudar a los clientes a adoptar prácticas seguras en línea y reconocer computadoras manipuladas, bloquear algunos tipos de contenido malicioso y, en general, contribuir a crear un entorno de comunicaciones seguro para sus clientes. Existen diversos modelos de alianzas público-privadas, como las establecidas entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios electrónicos. Muchas de estas alianzas se fundan en un intercambio de información basado en la claridad de las reglas, la confianza, el reducido número de miembros y la incentivación de la reciprocidad de los beneficios y la actuación. Algunos organismos sectoriales, como la Cyber Security Research Alliance, ofrecen plataformas para la colaboración entre el sector y los gobiernos en el ámbito de la ciberseguridad y la ciberdelincuencia.

37. Por último, es fundamental el desarrollo de la capacidad de los sistemas nacionales de aplicación de la ley y justicia penal. Aunque la mayoría de los países han comenzado a crear estructuras especializadas en la investigación de los delitos cibernéticos y de los delitos cuya persecución requiere pruebas electrónicas, muchos de ellos todavía no disponen de recursos suficientes o tienen problemas de capacidad. A medida que las pruebas digitales vayan ganando presencia en las investigaciones de delitos “convencionales”, las autoridades encargadas de hacer cumplir la ley deberán establecer distinciones claras entre los investigadores especializados en delitos cibernéticos y la capacidad digital de los laboratorios forenses y definir los correspondientes flujos de trabajo. Los funcionarios de primera línea encargados de la aplicación de la ley deberán adquirir y utilizar las competencias básicas necesarias para producir por ejemplo una imagen forense sólida de un dispositivo de almacenamiento electrónico.

38. A medida que los nuevos avances tecnológicos como las redes anonimizadoras, el encriptado de alto nivel y las monedas virtuales se conviertan en elementos habituales de los delitos cibernéticos, los investigadores se verán obligados también a adoptar nuevas estrategias. Las autoridades encargadas de hacer cumplir la ley pueden optar, por ejemplo, por reforzar sus alianzas con grupos de investigación académica que trabajen en el desarrollo de metodologías técnicas en ámbitos como la caracterización y la investigación de transacciones con monedas virtuales[33]. Los investigadores tal vez deberán explorar también la posibilidad de combinar la investigación en Internet y las técnicas forenses digitales con técnicas especiales de investigación como la vigilancia, las operaciones encubiertas, los informantes y la entrega vigilada en el caso de venta de mercancías ilícitas en línea. En conjunto, no cabe duda de que el desarrollo de la capacidad de los encargados de hacer cumplir la ley y de la justicia penal frente a la ciberdelincuencia será un proceso continuo, en vista del ritmo al que siguen evolucionando las innovaciones técnicas y delictivas.

---

[33] Véase, por ejemplo, Sarah Meiklejohn y otros, “A fistful of bitcoins: characterizing payments among men with no names”, en *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (Nueva York, ACM, 2013).

III. Tráfico de bienes culturales

A. Definición del problema

39. La protección de los bienes culturales se considera uno de los mayores retos a los que se enfrentan las políticas contemporáneas de justicia penal. Los bienes culturales son vistos actualmente como patrimonio no solo de los "países de origen", sino de toda la humanidad, que merece ser protegido y preservado en beneficio del conocimiento histórico y por su contribución a la constitución de las identidades culturales y el papel que desempeñan dentro de las prácticas sociales. Eso explica la creciente atención que las Naciones Unidas y muchas otras organizaciones internacionales han dedicado al fenómeno, y el compromiso de los Estados con el desarrollo y la aplicación de instrumentos jurídicos internacionales orientados a la protección de los bienes culturales.

40. La conducta característica que subyace al tráfico de bienes culturales resulta tal vez más fácil de definir que en el caso de los delitos cibernéticos, aunque la investigación encuentra dificultades importantes para definir el alcance y la escala del fenómeno. Esas dificultades, que son comunes a la investigación de muchos tipos de delincuencia organizada, incluyen la complejidad de las operaciones ilegales, la falta de capacidad y sensibilidad de los organismos encargados de la aplicación de la ley y la corrupción. Por otro lado, la proximidad de las actividades ilegales relacionadas con la exportación de bienes culturales robados a algunos elementos y métodos de funcionamiento del mercado legal de obras de arte y antigüedades en muchos países exige esfuerzos suplementarios. Las dificultades se ven exacerbadas cuando se trata de tráfico de bienes culturales procedentes de excavaciones ilícitas en yacimientos arqueológicos, ya que pueden plantearse enormes dificultades para identificar el lugar de origen de los objetos arqueológicos.

41. Se han llevado a cabo esfuerzos orientados a la recopilación de datos sobre el tráfico de bienes culturales, así como a la identificación de los métodos empleados por los grupos delictivos. Por ejemplo, un estudio realizado en 2009 utilizó información procedente de la base de datos Solución Comercial Integrada Mundial del Banco Mundial, que incluye datos sobre objetos de más de 100 años de antigüedad, con el fin de elaborar modelos empíricos explicativos del tráfico ilícito de obras de arte y antigüedades[34]. Dicho estudio mostraba la existencia de una fuerte correlación entre la corrupción y la probabilidad de que las exportaciones de antigüedades no estuviesen debidamente documentadas, claro indicador de la existencia de tráfico ilícito.

42. Otro enfoque consiste en determinar la configuración y dimensiones de los mercados ilícitos de bienes culturales. Algunos estudios han analizado el lado de la demanda de los mercados, centrándose en la venta de obras de arte y antigüedades en casas de subastas y tratando de determinar el origen y el historial de propietarios de estas piezas. Por ejemplo, un estudio de 2002 examinó más de 18.000 piezas de cerámica griega vendidas en casas de subastas de los Estados Unidos de América y del Reino Unido de Gran Bretaña e Irlanda del Norte entre 1954 y 1998, y puso de

[34] Raymond Fisman y 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* (1:3) (julio de 2009), págs. 82 a 96.

manifiesto que entre el 80% y el 90% de las piezas no tenían lugar de procedencia (es decir, la cadena de propietarios legítimos no podía remontarse hasta el hallazgo original)[35]. La falta de procedencia no es por sí misma prueba de tráfico ilícito, pero constituye un factor de riesgo importante. Otros estudios de los mercados ilícitos se centran en el lado de la oferta, a menudo a través del examen y la documentación de yacimientos arqueológicos saqueados. Algunos de estos estudios siguen métodos tradicionales de las ciencias sociales y de la conducta, como la realización de estudios de campo para documentar el estado de los yacimientos arqueológicos en determinados países. Más recientemente, el uso de potentes satélites comerciales ha permitido realizar estudios más frecuentes y exhaustivos de los yacimientos en busca de indicios de saqueo. Por ejemplo, una serie de estudios realizados en 2008 usaban imágenes digitales para documentar el grado de saqueo de los yacimientos arqueológicos iraquíes[36].

43. Algunos estudios también se han interesado por las diferentes fases de la cadena de suministro ilícito en el tráfico de bienes culturales. Algunos de ellos se han centrado en las personas que saquean yacimientos arqueológicos, como un estudio realizado en 2005 que abarcó a 400 personas dedicadas a esta actividad en Belice, y del que se concluyó que su principal móvil era la subsistencia económica más que la intención de hacer mal[37]. Otro estudio acerca de los saqueos ocurridos en el Iraq en 2003 y 2004 halló motivaciones económicas parecidas, aunque también observó la presencia de formas más organizadas de delincuencia en el control del acceso a los yacimientos y el asesinato de funcionarios de aduanas iraquíes que trataban de poner fin al saqueo[38]. Un estudio empírico más reciente dedicado a una red de tráfico de estatuas se basó en entrevistas de historia oral realizadas en el marco de un estudio de campo sobre criminología etnográfica en Camboya y Tailandia, y abarcó los niveles de organización de las actividades ilícitas conexas[39].

44. Algunos estudios han debatido la implicación de la delincuencia organizada o de la delincuencia organizada transnacional en los mercados ilícitos de bienes culturales. Un estudio elaboró un metaanálisis de otros estudios sobre el tráfico de bienes culturales previamente publicados y llegó a la conclusión de que era preferible determinar cómo se producía el tráfico e identificar cuáles eran las funciones y las relaciones entre los distintos autores dentro de cada red, en lugar de dar por supuesto que todas las formas de tráfico de bienes culturales encajaban en la

---

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

[36] Véase Elizabeth Stone, “Patterns of Looting in Southern Iraq”, *Antiquity,* vol. 82, núm. 315 (marzo de 2008), págs. 125 a 138.

[37] David Matsuda, “Subsistence Diggers”, en *Who Owns the Past? Cultural Policy, Cultural Property, and the Law*, Kate Fitz Gibbon, ed. (New Brunswick, Nueva Jersey, Rutgers University Press, 2005), págs. 255 a 268.

[38] Joanne Farchakh-Bajjaly, “Who are the Looters at Archaeological Sites in Iraq?”, en *Antiquities Under Siege: Cultural Heritage Protection After the Iraq War*, Lawrence Rothfield, ed. (Washington DC, Altamira Press, 2008), págs. 49 a 56.

[39] Simon Mackenzie y Tess Davis, “Temple looting in Cambodia: anatomy of a statue trafficking network”, *British Journal of Criminology*, vol. 54, núm. 5 (septiembre de 2014), págs. 722 a 740.

categoría de delincuencia organizada[40]. Otro estudio aplicaba el paradigma de la red para explicar la estructura relativamente flexible del comercio ilícito de bienes culturales, y alentaba a realizar nuevos estudios sobre la estructura organizativa de esta clase de tráfico[41]. Otro centraba su atención en la cadena de coautores del delito, en el marco de un estudio monográfico del tráfico de bienes culturales, e identificaba sus funciones, interrelaciones y conductas parcialmente jerarquizadas[42].

B. Respuestas al tráfico de bienes culturales

45. Se han aprobado varios instrumentos internacionales para dar respuesta al tráfico de bienes culturales. El objetivo primario de la Convención para la Protección de los Bienes Culturales en caso de Conflicto Armado (1954) y sus protocolos adicionales era la prevención y la sanción de los daños causados a los bienes culturales en el curso de las guerras. Otros instrumentos internacionales abordan las importaciones, las exportaciones y la transferencia de propiedad ilícitas de bienes culturales en cualquier circunstancia. Algunos de estos instrumentos son la Convención sobre las Medidas que Deben Adoptarse para Prohibir e Impedir la Importación, la Exportación y la Transferencia de Propiedad Ilícitas de Bienes Culturales y el Convenio sobre los Bienes Culturales Robados o Exportados Ilícitamente. El compromiso internacional con la salvaguardia del patrimonio cultural también encontró su expresión en otros instrumentos como la Convención sobre la Protección del Patrimonio Cultural Subacuático. A nivel regional, la Convención europea sobre las infracciones relativas a los Bienes Culturales se abrió a la firma en 1985, aunque todavía no ha entrado en vigor.

46. Un instrumento no vinculante que resulta de interés en el contexto del derecho penal es el tratado modelo para la prevención de los delitos contra los bienes muebles que forman parte del patrimonio cultural de los pueblos[43]. Algunas de las disposiciones de este tratado modelo pueden servir de base para la elaboración de disposiciones normativas dirigidas a combatir el tráfico de bienes culturales. En su resolución 2003/29, el Consejo Económico y Social alentó a los Estados Miembros a que estudiaran el tratado modelo, si correspondía y conforme a su derecho interno, al suscribir acuerdos pertinentes con otros Estados[44].

---

[40] Jessica Dietzler, “On ‘organized crime’ in the illicit antiquities trade: moving beyond the definitional debate”, *Trends in Organized Crime*, vol. 16, núm. 3 (septiembre de 2013), págs. 329 a 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, núm. 2 (mayo de 2013), págs. 113 a 153.

[42] Mackenzie y Davis, “Temple looting in Cambodia: anatomy of a statue trafficking network”.

[43] *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, La Habana, 27 de agosto a 7 de septiembre de 1990: informe preparado por la Secretaría* (publicación de las Naciones Unidas, núm. de venta S.91.IV.2), cap. I, secc. B.1, anexo.

[44] Véase también la Directriz 14 de las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos. Es preciso señalar también que, en su resolución 68/186, la Asamblea General solicitó a la UNODC que continuara su examen del tratado modelo, teniendo presentes las opiniones y observaciones formuladas por los Estados Miembros, y solicitó a los Estados Miembros y a las

47. La enorme difusión y la complejidad del tráfico de bienes culturales son cada vez más reconocidas actualmente, a nivel tanto internacional como nacional. Se considera que el tráfico de bienes culturales y delitos conexos constituyen un sector de la delincuencia en constante crecimiento, y cada vez más atractivo para las organizaciones delictivas nacionales y transnacionales. Esos factores han llevado a los Estados Miembros a negociar y adoptar otro instrumento, las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos, que constituyen un marco útil para orientar a los Estados Miembros en la elaboración y el fortalecimiento de políticas, estrategias, leyes y mecanismos de cooperación en el ámbito de la protección contra el tráfico de bienes culturales y otros delitos conexos.

48. Desde 2000, los organismos intergubernamentales han expresado una preocupación creciente por el tráfico de bienes culturales. Al aprobar la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la Asamblea General declaró en el preámbulo de su resolución 55/25 su firme convicción de que la Convención contra la Delincuencia Organizada constituiría un instrumento eficaz y el marco jurídico necesario para la cooperación internacional con miras a combatir, entre otras cosas, los delitos contra el patrimonio cultural[45].

49. Posteriormente, el Consejo Económico y Social, en sus resoluciones 2004/34 y 2008/23, expresó su alarma por la participación de grupos delictivos organizados en el tráfico de bienes culturales, y reafirmó la necesidad de la cooperación internacional para combatirlo. En su resolución 2010/19, el Consejo Económico y Social consideró que la Convención contra la Delincuencia Organizada y la Convención de las Naciones Unidas contra la Corrupción se deberían aplicar plenamente para reforzar la lucha contra el tráfico de bienes culturales, incluso estudiando la posibilidad de elaborar otros instrumentos normativos, cuando procediera. Durante su quinto período de sesiones, en 2010, la Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada aprobó la resolución 5/7, en la que instó a los Estados parte a que utilizaran la Convención para cooperar ampliamente en la prevención y represión de los delitos contra los bienes culturales, especialmente en lo referente a la devolución de esos bienes o del producto de dichos delitos a sus legítimos propietarios, con arreglo a lo dispuesto en el artículo 14, párrafo 2, de la Convención. Por otro lado, la Asamblea General, en sus resoluciones 66/180 y 68/186 invitó a los Estados Miembros a que estudiaran, según procediera, la posibilidad de revisar sus marcos jurídicos con el fin de prestar la más amplia cooperación internacional posible para abordar la cuestión del tráfico de bienes culturales en todos sus aspectos, e invitó también a que tipificaran como delito grave, tal como se define en el artículo 2 de la Convención contra la Delincuencia Organizada, el tráfico de bienes culturales, como el robo y el saqueo en yacimientos arqueológicos y otros sitios culturales con miras a utilizar plenamente dicha Convención en aras de una cooperación internacional amplia para combatir el tráfico de bienes culturales en todas sus formas y aspectos y los delitos conexos. En cumplimiento de estas

---

organizaciones internacionales competentes que todavía no lo hubieran hecho que presentaran a la Secretaría sus observaciones sobre el tratado modelo.

[45] El documento CTOC/COP/2010/12 contiene un análisis de las cuestiones relacionadas con la aplicabilidad de la Convención en este terreno.

resoluciones los Estados Miembros han elaborado las Directrices Internacionales antes mencionadas.

50. Las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos contienen capítulos dedicados a los siguientes temas: a) las estrategias de prevención del delito (que abarca la reunión de información y datos, la función de las instituciones culturales y el sector privado, la vigilancia del mercado de bienes culturales, las importaciones y exportaciones, los yacimientos arqueológicos y la educación y concienciación); b) las políticas de justicia penal (que abarca la adhesión a los tratados internacionales pertinentes y la aplicación de dichos tratados, la tipificación de determinadas conductas nocivas o el establecimiento de infracciones administrativas, la responsabilidad de las empresas, la incautación y el decomiso y las medidas de investigación); c) la cooperación internacional (que abarca cuestiones relacionadas con la base jurisdiccional, la extradición, la incautación y el decomiso, la cooperación entre las autoridades encargadas de hacer cumplir la ley y las encargadas de la investigación y la devolución, restitución o repatriación de bienes culturales); y d) el ámbito de aplicación de las directrices, que será toda situación, incluidas las circunstancias excepcionales, que propicie el tráfico de bienes culturales y delitos conexos.

51. Las respuestas al tráfico de bienes culturales dependen en gran medida de la cooperación y coordinación entre Estados, así como de las alianzas público-privadas. Dicha cooperación y colaboración se podrá traducir, por ejemplo, en la inclusión de información exhaustiva en los inventarios y bases de datos, que pueden ser herramientas importantes para actuar con la debida diligencia en relación con la procedencia antes de que un artefacto cultural sea vendido en el mercado legítimo, incluidas las casas de subastas, y facilitar las investigaciones de posibles casos de robo y tráfico. Además del establecimiento de inventarios y bases de datos nacionales, la base de datos de la INTERPOL sobre obras de arte robadas[46] combina descripciones específicas e imágenes de aproximadamente 43.000 objetos, lo que puede resultar especialmente útil en casos transnacionales. Las trece “listas rojas”[47] ya publicadas por el Consejo Internacional de Museos, organización no gubernamental internacional, clasifican por categorías los objetos arqueológicos u obras de arte en situación de riesgo en las zonas más vulnerables del mundo, como el Afganistán, Haití y la República Árabe Siria, para prevenir su venta o exportación ilegal. El Art Loss Register[48] es una importante base de datos privada de obras de arte, antigüedades y artículos de coleccionista perdidos y robados. También contiene datos de obras que no han sido robadas, lo que puede tener un efecto disuasorio para ladrones potenciales y contribuir a su recuperación[49] en caso de que fueran robados.

---

[46] Disponible en http://www.interpol.int/Crime-areas/Works-of-art/Database.

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

[48] Disponible en http://www.artloss.com/en.

[49] Cabe observar que el artículo 5 b) de la Convención sobre las Medidas que Deben Adoptarse para Prohibir e Impedir la Importación, la Exportación y la Transferencia de Propiedad Ilícitas de Bienes Culturales dispone que los Estados partes deben establecer y mantener al día, a partir de un inventario nacional de protección, la lista de los bienes culturales importantes, públicos y privados, cuya exportación constituiría un empobrecimiento considerable del patrimonio cultural nacional. Como medida preventiva, la Directriz 1 de las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y

52. La importancia de las respuestas coordinadas se plasma también en la iniciativa conjunta de sensibilización de la UNODC, la Organización Mundial del Turismo y la UNESCO que insta a los viajeros a apoyar la lucha contra diversas modalidades de tráfico, incluido el tráfico de bienes culturales[50]. Otro ejemplo útil de la importancia de la cooperación entre organizaciones intergubernamentales, organismos nacionales y el sector privado puede encontrarse en el establecimiento por el Consejo Internacional de Museos del Observatorio Internacional sobre el Tráfico Ilícito de Bienes Culturales[51], plataforma de colaboración donde las personas y las organizaciones interesadas pueden encontrar información y recursos.

IV. Conclusiones y recomendaciones

53. Por más que la ciberdelincuencia y el tráfico puedan diferir en cuanto al objeto primario del delito, no cabe duda de que los nuevos elementos impulsores subyacentes, como la globalización y el surgimiento de las nuevas tecnologías, desempeñan un papel central en la aparición de mercados ilícitos en uno y otro ámbito. El desarrollo de esas raíces y elementos impulsores puede conllevar un aumento de la capacidad de ambos tipos delictivos para expandirse y causar cada vez más pérdidas y daños. En el caso particular de la ciberdelincuencia, las dimensiones del mercado delictivo –en ámbitos tales como la extorsión en línea, las ventas ilícitas en línea y la violación y venta de datos– no dejan de crecer a medida que aumenta la proporción de la población mundial que se conecta a Internet. Saber anticiparse y prepararse ante la evolución futura de los mercados ilícitos en el ámbito de la ciberdelincuencia y del tráfico de bienes culturales es crucial para el diseño de respuestas eficaces.

54. Este proceso debe comenzar por una investigación sistemática y por la elaboración de estadísticas oportunas, fiables y accesibles sobre ambos tipos de delitos. Tal como se señala en el informe del Grupo Asesor de Expertos Independientes sobre la Revolución de los Datos para el Desarrollo Sostenible[52], hace falta un consenso mundial sobre los datos que permita compartir y emplear la tecnología y la innovación para el bien común, lo que incluye la creación de una red mundial de innovación en materia de datos. La misma idea debe aplicarse también a la comprensión y la medición de problemas emergentes a nivel mundial ligados a la delincuencia, como la ciberdelincuencia y el tráfico de bienes culturales.

55. Otras respuestas a la ciberdelincuencia y el tráfico de bienes culturales podrían ser las siguientes:

a) Los Estados Miembros pueden considerar la posibilidad de fortalecer su capacidad para llevar registros de delitos conexos e intercambiar información a nivel regional e internacional acerca de la actividad de los grupos delictivos

---

Otros Delitos Conexos indica también que “los Estados deberían considerar la posibilidad de establecer y mantener, según proceda, inventarios o bases de datos de los bienes culturales con el fin de protegerlos contra el tráfico. El hecho de que los bienes culturales no estén registrados en dichos inventarios en modo alguno los excluirá de la protección (…)”.

[50] Más información disponible en http://www.bearesponsibletraveller.org.

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

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

organizados, los *modus operandi* de esos grupos y las técnicas empleadas en la identificación de las distintas formas de ciberdelincuencia y tráfico de bienes culturales;

b) La interacción entre las empresas del sector privado, ya se trate de proveedores de servicios en Internet, bancos, empresas de distribución y logística global, museos o casas de subastas, y las instituciones públicas como las autoridades encargadas de hacer cumplir la ley y de la justicia penal, debería encauzarse a través de alianzas público-privadas que promuevan la confianza y el diálogo abierto. De modo más general, las respuestas normativas del Estado que vayan más allá del derecho penal e incentiven la participación activa del sector privado en la prevención del delito pueden ser útiles para crear un entorno sensible a las nuevas amenazas y propicio para detectarlas y combatirlas;

c) Los Estados Miembros pueden considerar la posibilidad de revisar y fortalecer su marco nacional de prevención y lucha contra el tráfico de bienes culturales, incluso en circunstancias de especial vulnerabilidad de los bienes culturales, recurriendo por ejemplo a las Directrices Internacionales sobre las Respuestas de Prevención del Delito y Justicia Penal al Tráfico de Bienes Culturales y Otros Delitos Conexos. En el ámbito de la ciberdelincuencia, los Estados Miembros pueden considerar la posibilidad de garantizar un enfoque jurídico equilibrado que tipifique como delitos específicos los actos básicos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos y, al mismo tiempo, revisar la aplicabilidad de otros delitos de carácter general, como el robo, el fraude, la falsificación y los daños personales, a los actos cometidos en línea;

d) Los Estados Miembros tal vez necesiten encontrar formas de promover la cooperación internacional en asuntos penales. En la esfera de los delitos cibernéticos, eso puede suponer, en particular, estudiar las posibilidades de agilizar los procedimientos formales de asistencia judicial recíproca y fortalecer la cooperación entre las autoridades encargadas de hacer cumplir la ley, y mantener un diálogo multilateral continuo sobre el acceso transnacional a datos informáticos. En lo que respecta al tráfico de bienes culturales, eso podría requerir un incremento de los esfuerzos destinados a la investigación y la persecución de redes delictivas mediante el intercambio de información entre cuerpos de investigación nacionales especializados;

e) Es preciso que las investigaciones y las estadísticas, las alianzas público-privadas, los marcos legislativos y los mecanismos de cooperación internacional dispongan de capacidad efectiva a nivel nacional. La asistencia técnica y la cooperación son importantes para hacer posible el intercambio de buenas prácticas investigadoras y experiencia, así como para la difusión de nuevas técnicas. En la esfera de la ciberdelincuencia, los Estados Miembros podrían potenciar el intercambio de nuevos enfoques para la investigación de complejos fraudes financieros basados en Internet, el tráfico de drogas en línea, o el uso de monedas virtuales para el blanqueo de dinero, lo que permitiría a las autoridades encargadas de hacer cumplir la ley de múltiples países adquirir rápidamente las competencias necesarias para hacer frente a las nuevas amenazas. En relación con el tráfico de bienes culturales, los Estados Miembros podrían potenciar la capacidad de los servicios de fronteras y aduanas para identificar bienes culturales objeto de tráfico, explorar las conexiones entre los marcos nacionales para combatir el blanqueo de

dinero y el tráfico de bienes culturales, e identificar e intercambiar buenas prácticas en todos los ámbitos de las respuestas de prevención del delito y justicia penal al tráfico de bienes culturales;

f) La UNODC debería seguir prestando asistencia técnica a los Estados Miembros con el fin de fortalecer las respuestas de prevención del delito y justicia penal a las formas nuevas y emergentes de delincuencia, entre ellas la ciberdelincuencia y el tráfico de bienes culturales y delitos conexos, a petición de las organizaciones internacionales pertinentes y en coordinación con ellas. Los Estados Miembros podrían considerar con carácter prioritario la posibilidad de asignar fondos a estos fines;

g) Los Estados Miembros podrían adoptar un enfoque holístico en relación con la ciberdelincuencia y el tráfico de bienes culturales, que tenga en cuenta tanto los *modus operandi* y las amenazas delictivas actuales como su posible evolución futura. Las respuestas deberán basarse cada vez más en la cooperación global, la participación de múltiples interesados y el uso de la tecnología, como bases de datos y plataformas de comunicación seguras.