Naciones Unidas CTOC/COP/WG.3/2015/2

Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

Distr. general
18 de agosto de 2015
Español
Original: inglés

Grupo de Trabajo sobre Cooperación Internacional
Viena, 27 y 28 de octubre de 2015
Tema 2 del programa provisional*
Reunión e intercambio de pruebas electrónicas

Reunión e intercambio de pruebas electrónicas

Documento de antecedentes preparado por la Secretaría

I. Introducción

1. Los delitos que entrañan pruebas electrónicas presentan problemas singulares a las autoridades encargadas de darles respuestas adecuadas en el plano interno (legisladores, investigadores, fiscales y jueces) y a nivel de la cooperación internacional.

2. En términos generales, las pruebas electrónicas pueden incluir cualesquiera datos generados o memorizados en formato digital cuando se utiliza una computadora. Abarcan la información introducida manualmente por una persona en un dispositivo electrónico, la información generada a solicitud de una persona o en una transacción por computadora, en la que un dispositivo electrónico genera información como autómata, o información producida y almacenada en un dispositivo que procesa la información contenida en su matriz. Por consiguiente, las pruebas electrónicas son cualquier información registrada, generada o archivada en bases de datos, sistemas operativos, programas de aplicaciones, modelos generados por computadora que extrapolan resultados, mensajes de voz y correo electrónico e incluso instrucciones inactivas contenidas en la memoria de una computadora[1].

3. El presente documento ha sido preparado por la Secretaría para proporcionar información básica sobre los principales conceptos y aspectos relacionados con las pruebas electrónicas y ayudar al Grupo de Trabajo a examinar el tema pertinente del programa de su reunión.

---

* CTOC/COP/WG.3/2015/1.

[1] Ireland Law Reform Commission, "Documentary and Electronic Evidence", Consultation paper, diciembre de 2009, pág. 8.

V.15-05871 (S) 110915 110915

II. Reunión e intercambio de pruebas electrónicas: aspectos que hay que considerar y respuestas en los planos nacional e internacional

4. La reunión y el intercambio de pruebas electrónicas están estrechamente vinculados, y de ahí que la legislación nacional y los acuerdos o arreglos regionales e internacionales a menudo establezcan facultades de investigación para reunir pruebas electrónicas y mecanismos de cooperación para intercambiarlas.

A. Reunión de pruebas electrónicas

1. Marcos jurídicos nacionales

5. El derecho procesal penal tradicional normalmente contiene disposiciones relativas a la reunión de pruebas y su admisibilidad. En el caso de las pruebas en forma electrónica, los datos informáticos y los archivos electrónicos pueden alterarse fácilmente. Por ello, la reunión de pruebas electrónicas y su gestión deben garantizar su integridad, autenticidad y continuidad durante todo el período comprendido entre su obtención y su utilización en un juicio.

a) Facultades legales para reunir y gestionar pruebas electrónicas

6. Las facultades nacionales de investigación desempeñan un papel fundamental en la reunión de pruebas electrónicas. Como se indica en el estudio de la UNODC sobre el delito cibernético, los Estados podrían promulgar legislación procesal que otorgara a las autoridades policiales pertinentes atribuciones para llevar a cabo investigaciones efectivas y reunir pruebas electrónicas. Las facultades de investigación pueden abarcar la aplicación de las competencias procesales tradicionales, competencias generales de investigación interpretadas en sentido lato, competencias generales de investigación adaptadas para que sean aplicables a toda una gama de medidas específicas en el ámbito cibernético y el ejercicio de amplios poderes de investigación para obtener pruebas electrónicas[2].

7. Como se señala también en el estudio sobre el delito cibernético, el análisis de la base legal de las facultades de investigación que se utilizan en relación con los delitos que entrañan pruebas electrónicas muestra que los enfoques a nivel nacional varían considerablemente. Esos enfoques guardan relación en primer lugar con la medida en que los poderes “tradicionales” pueden interpretarse en el sentido de que son aplicables a datos intangibles y la medida en que existe la autoridad legal para adoptar medidas particularmente intrusivas, como investigaciones forenses a distancia.

8. No obstante, si bien las facultades legales varían, parece existir un grado considerable de consenso entre los Estados que aportaron información para el estudio sobre el delito cibernético respecto de los tipos de medidas de investigación que deberían estar disponibles para reunir pruebas electrónicas. Esas medidas

[2] UNODC, *Comprehensive Study on Cybercrime: Draft — 2013*, estudio preparado por la UNODC para su examen por el Grupo de Expertos Encargado de realizar un Estudio Exhaustivo del Delito Cibernético (www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf), capítulo 5, pág. 125.

pueden consistir en la rápida conservación de datos informáticos; requerimientos de datos de contenido almacenados; requerimientos de datos de tráfico almacenados; requerimientos de información sobre suscriptores; la recopilación en tiempo real de datos sobre el contenido; la recopilación en tiempo real de datos de tráfico; la inspección de equipo o datos informáticos; la incautación de equipo o datos informáticos; el acceso transfronterizo a un sistema o datos informáticos; y el empleo de herramientas de análisis forense a distancia[3].

9. La importancia que la cooperación con otras entidades pertinentes, incluso del sector privado, reviste para que las fuerzas de orden puedan investigar y reunir pruebas electrónicas en relación con el delito cibernético de manera eficaz ha aumentado particularmente en los últimos años. En general, los proveedores de servicios de Internet desempeñan un papel importante en lo que respecta a la accesibilidad de las pruebas electrónicas. Las leyes nacionales de privacidad también pueden influir en la capacidad de esos proveedores de compartir información con las autoridades pertinentes durante la investigación. A título de ejemplo, los Estados pueden hacer observar restricciones en cuanto a los datos a los que es posible tener acceso, imponer plazos y tener requisitos de "causa razonable" y supervisión fiscal y judicial[4]. De resultas de las protecciones basadas en la privacidad establecidas en la legislación nacional, los proveedores de servicios de Internet pueden estar obligados a no divulgar información relativa a los datos personales de los suscriptores, los datos de contenido y los datos de tráfico. Aparte de las leyes nacionales, el derecho internacional de los derechos humanos establece normas específicas sobre los derechos de privacidad de las personas sujetas a investigaciones policiales.

10. Las "Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia" del Consejo de Europa se adoptaron en respuesta a la importancia de esos proveedores para la reunión de pruebas electrónicas. La finalidad de las directrices es ayudar a las fuerzas del orden y a los proveedores de servicios a organizar su cooperación en la lucha contra la ciberdelincuencia. Se pretende que las directrices sean flexibles y se apliquen en todos los países de conformidad con la legislación nacional y respetando los derechos fundamentales de los ciudadanos. En ellas se alienta a las autoridades responsables de velar por el cumplimiento de la ley y a los proveedores de servicios de Internet, entre otras cosas, a participar en el intercambio de información; promover una cultura de cooperación; establecer procedimientos por escrito para la cooperación mutua; contemplar la posibilidad de crear alianzas oficiales; y proteger los derechos fundamentales de los ciudadanos[5].

---

[3] En el archivo de datos sobre el delito cibernético (http://cybrepo.unodc.org) y el portal SHERLOC (http://sherloc.unodc.org) pueden encontrarse ejemplos de leyes nacionales sobre esas medidas de investigación.

[4] Estudio sobre el delito cibernético, capítulo 5, pág. 134.

[5] Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia" disponibles en http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/567_prov-d-guidelines_provisional2%20_3%20April%202008_final_spanish.pdf.

b) Fomento de la capacidad de los sistemas de aplicación de la ley y justicia penal para gestionar pruebas electrónicas

11. Las pruebas electrónicas son frágiles por naturaleza. Pueden ser alteradas, dañadas o destruidas por una gestión o un examen inadecuado. Por esta razón, deben adoptarse precauciones especiales para documentar, reunir, conservar y analizar este tipo de pruebas. De lo contrario, pueden volverse inutilizables o llevar a una conclusión inexacta.

12. Por ello, 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.

13. 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[6]. 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[7].

---

[6] 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 (Nueva York, Reunión de Coordinación Anual, 2013).

[7] 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, documento de antecedentes preparado por la Secretaría para el seminario 3: El fortalecimiento de las respuestas de prevención del delito y justicia penal 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, A/CONF.222/12, párrs. 37 y 38.

c) Enfoques nacionales de la función de las estructuras y dependencias especializadas en delitos cibernéticos

14. La especialización de los organismos nacionales de aplicación de la ley en la investigación de los delitos cibernéticos o los delitos que entrañan pruebas electrónicas es cada vez más frecuente y desempeña un papel fundamental de facilitación de los procesos de reunión, análisis e intercambio de pruebas electrónicas. Esa especialización está vinculada principalmente a la naturaleza particular del delito cibernético, que plantea problemas específicos relacionados con las definiciones de delitos, la aplicación de leyes y la reunión y el análisis de pruebas. El nivel de capacidad y conocimientos técnicos de los organismos encargados de aplicación de la ley tendrá por lo tanto un efecto directo en la eficacia de las respuestas en materia de prevención del delito y justicia penal a la ciberdelincuencia[8]. Además, 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"[9]. Como resultado de ello, también es cada vez más necesario que los organismos de aplicación de la ley, de todos los niveles, tanto locales como nacionales, cuenten por lo menos con las capacidades básicas para investigar los delitos cibernéticos.

15. El sector que se citaba con más frecuencia como necesitado de "intervenciones de asistencia técnica" en el estudio sobre el delito cibernético es el de técnicas generales de investigación de delitos cibernéticos. El 60% de los países que necesitaban asistencia señalaron que la necesitaban los organismos encargados de aplicar la ley[10]. Los Estados que aportaron información para el estudio sobre el delito cibernético señalaron también que, en muchos casos, las comisarías de policía remitían los casos de ciberdelincuencia al máximo órgano especializado de aplicación de la ley a nivel nacional[11].

16. Las dependencias o estructuras de los organismos especializados en delitos informáticos pueden ayudar a los Estados a concentrar en un solo lugar sus limitados recursos para desarrollar técnicas de investigación especializadas y reunir y analizar adecuadamente las pruebas electrónicas, incluso llevando a cabo exámenes forenses digitales. Al mismo tiempo, esas dependencias o estructuras pueden impartir capacitación a los órganos de orden público locales, coordinar las respuestas nacionales a la ciberdelincuencia, facilitar la cooperación entre los participantes en las investigaciones y centrarse en las formas de delincuencia cibernética que pueden ser motivo de especial preocupación para un Estado, como, entre otras, el abuso de menores por Internet, los delitos relacionados con la identidad y los fraudes y las estafas por Internet.

---

[8] Estudio sobre el delito cibernético, capítulo 5, pág. 152.
[9] Véase la nota 7 *supra*, A/CONF.222/12, párr. 16.
[10] Estudio sobre el delito cibernético, resumen, pág. xxiii.
[11] Estudio sobre el delito cibernético, capítulo 5, pág. 118.

d) Admisibilidad de pruebas electrónicas en los tribunales

17. Lo ideal sería que, una vez se hubieran reunido e intercambiado pruebas electrónicas, estas fueran admisibles en los procedimientos penales. El derecho probatorio se ha basado tradicionalmente en documentos escritos, aunque los testimonios orales y los objetos físicos siempre han formado parte de las actuaciones judiciales. Sin embargo, la importancia cada vez mayor de las pruebas electrónicas en los procesos penales plantea problemas hasta ahora desconocidos y de ahí que el informe sobre la delincuencia cibernética constituyera un proceso de examen encaminado a reflejar las orientaciones de las legislaciones nacionales con respecto a la admisibilidad de esas pruebas en los tribunales penales.

18. En ese contexto, el 85% de los países que aportaron información señalaron que las pruebas electrónicas eran admisibles en un proceso penal. La mayoría de los países que admiten pruebas electrónicas informaron de que se les daba el mismo trato que a las pruebas materiales. Menos del 40% de los países comunicaron la existencia de una distinción jurídica entre pruebas electrónicas y pruebas materiales. Muy pocos países informaron de la existencia de leyes especiales relacionadas con las pruebas electrónicas. Los que lo hicieron, señalaron que las leyes se referían a cuestiones como las presunciones legales de propiedad y autoría de datos y documentos electrónicos y las circunstancias en que las pruebas electrónicas podían considerarse auténticas[12].

2. Cooperación internacional

19. Los delitos que entrañan pruebas digitales plantean desafíos singulares en materia de cooperación internacional. Debido al carácter volátil de la prueba electrónica, la cooperación internacional en asuntos penales en la esfera de los delitos cibernéticos requiere una respuesta pronta y la habilidad de solicitar diligencias investigativas especializadas, como la conservación y producción de datos por proveedores del sector privado. Algunos problemas comunes para solicitar esos datos a otra jurisdicción son la demora en la respuesta a solicitudes, la falta de dedicación y flexibilidad de la autoridad a la que se solicitan pruebas, la forma de presentar las pruebas a la jurisdicción requirente y la cuestión de si pueden utilizarse en procesos penales, así como las diferencias entre las jurisdicciones en cuanto a las definiciones de qué constituye un delito[13].

20. Si bien existen varias formas de cooperación oficiosa entre las autoridades encargadas de hacer cumplir la ley, incluidas redes accesibles de manera ininterrumpida, los países siguen utilizando en gran medida formas tradicionales de asistencia judicial oficial para obtener pruebas digitales de otras jurisdicciones, en particular instrumentos bilaterales de asistencia judicial recíproca, y más del 70% de ellos se valen de solicitudes oficiales de asistencia judicial recíproca[14]. El tiempo de respuesta a estas solicitudes de asistencia judicial recíproca en investigaciones de delitos cibernéticos suele ser de alrededor de 150 días. Este plazo muchas veces

---

[12] Estudio sobre el delito cibernético, capítulo 6, págs. 165 a 167.

[13] UNODC, estudio comparativo titulado “Current practices in electronic surveillance in the investigation of serious and organized crime”, pág. 9 (www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf).

[14] Estudio sobre el delito cibernético, resumen, pág. xxv.

supera el período de conservación de datos de los proveedores de servicios o permite a los autores del delito destruir pruebas digitales decisivas.

21. En consecuencia, la cooperación internacional eficaz en casos que entrañan pruebas digitales exige mecanismos para lograr rápidamente la conservación de datos mientras se examina la posibilidad de adoptar otras medidas investigativas. La cooperación internacional en casos que entrañan pruebas digitales también puede mejorarse mediante enfoques comunes de formulación de solicitudes de tipos específicos de pruebas, incluidos pruebas de la red, registros de conexión e imágenes forenses.

22. 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, el acceso transfronterizo a datos informáticos almacenados, con consentimiento o cuando sean de acceso público, y las solicitudes urgentes de asistencia mutua.

23. Por ejemplo, en virtud del Convenio sobre la Ciberdelincuencia del Consejo de Europa, unos puntos de contacto disponibles las veinticuatro horas del día, siete días a la semana, han de facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas: i) el asesoramiento técnico; ii) la conservación de datos; y iii) la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

24. Diversos acuerdos internacionales se refieren a los aspectos relacionados con la reunión de pruebas electrónicas. A título de ejemplo, en virtud de las disposiciones sobre procedimiento del Convenio sobre la Ciberdelincuencia del Consejo de Europa los poderes y procedimientos en él previstos se aplicarán a la obtención de pruebas electrónicas de un delito.

25. El proyecto de ley modelo sobre ciberseguridad (2011) del Mercado Común para África Oriental y Meridional (COMESA) contiene disposiciones relativas a los proveedores de servicios de Internet. Esas disposiciones incluyen obligaciones de vigilancia (art. 17); el suministro voluntario de información (art. 17 b)); notificaciones de detección (art. 16); la responsabilidad de los proveedores de acceso (art. 12); el almacenamiento en caché (art. 13); el hospedaje de sitios web (art. 14); y los proveedores de hiperenlaces y buscadores (art. 15). Además, la Directiva 2000/31/CE de la Unión Europea y los modelos de textos legislativos de la Unión Internacional de Telecomunicaciones, la Comunidad del Caribe y la Unión de Telecomunicaciones del Caribe sobre: i) el delito cibernético y electrónico y ii) las pruebas electrónicas, contienen disposiciones similares, si bien en menor cantidad que el proyecto de ley modelo de la COMESA.

26. Los organismos encargados de hacer cumplir la ley pueden mantener una cooperación oficiosa para reunir pruebas electrónicas de otras jurisdicciones. Esa cooperación puede facilitar diversas medidas para obtener pruebas extraterritoriales, tales como la búsqueda e incautación; la conservación de datos informáticos, requerimientos de datos informáticos; la recopilación de datos en

tiempo real; el uso de herramientas de análisis forense a distancia; y el acceso directo de los órganos de orden público a datos extraterritoriales[15].

27. 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[16] y el Centro Europeo contra la Delincuencia Informática (EC3)[17] de la Oficina Europea de Policía (Europol) en tareas de coordinación y apoyo de las investigaciones transnacionales 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.

28. La computación en la nube también plantea nuevas dificultades para la cooperación internacional porque cada vez más servicios informáticos están siendo transferidos a servidores y centros de datos distribuidos geográficamente, lo que hace difícil determinar dónde se "encuentran" las pruebas electrónicas[18]. A título de ejemplo, un usuario de Google puede acceder a datos almacenados o tratados en América del Norte, Asia Sudoriental o Europa septentrional u occidental[19].

B. Intercambio de pruebas electrónicas

1. Marcos jurídicos nacionales

29. Algunos Estados han promulgado legislación interna que regula el intercambio de pruebas mediante la cooperación internacional. A título de ejemplo, muchos Estados tienen una legislación nacional sobre asistencia recíproca en asuntos penales que también puede utilizarse para intercambiar pruebas electrónicas.

2. Cooperación internacional

30. Los Estados pueden concertar acuerdos bilaterales, regionales e internacionales para facilitar el intercambio interjurisdiccional de pruebas electrónicas. Esos acuerdos pueden contener disposiciones relativas a la asistencia para la conservación de datos informáticos; la asistencia para la incautación, recogida y divulgación de datos informáticos y el acceso a ellos; el acceso transfronterizo a datos informáticos; el suministro de información no solicitada y el intercambio de información; y solicitudes de asistencia judicial recíproca en general[20]. Las disposiciones de esos acuerdos constituyen fuentes principales de derecho que se refieren tanto a los derechos como a las obligaciones de las partes en ellos y, por lo tanto, les imponen condiciones jurídicas vinculantes. Sin embargo, no todos los Estados exigen que exista un tratado oficial de cooperación judicial para intercambiar pruebas electrónicas y pueden, en lugar de ello, prestar asistencia sobre la base de la reciprocidad o de la cortesía.

---

[15] Estudio sobre el delito cibernético, capítulo 5, págs. 126 a 133.
[16] www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation.
[17] www.europol.europa.eu/ec3.
[18] Estudio sobre el delito cibernético, capítulo 7, pág. 216.
[19] Estudio sobre el delito cibernético, capítulo 7, págs. 216 y 217.
[20] Estudio sobre el delito cibernético, anexo 3, págs. 273 y 274.

31. Un examen de los acuerdos regionales e internacionales pone de manifiesto las diversas formas en que los Estados pueden intercambiar pruebas electrónicas. Esas formas de cooperación abarcan los principios generales de cooperación internacional; la asistencia judicial recíproca en general; los mecanismos de asistencia rápida; la asistencia para la conservación de datos informáticos; la asistencia para la incautación, recogida y divulgación de datos informáticos y el acceso a ellos; el acceso transfronterizo a datos; y el suministro e intercambio de información por iniciativa propia. Los siguientes acuerdos contemplan varias de las formas de cooperación antes mencionadas:

Naciones Unidas, Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000);

Comunidad de Estados Independientes, Acuerdo sobre la Cooperación para luchar contra el delito en la esfera de la información computadorizada (2001);

Consejo de Europa, Convenio sobre la Ciberdelincuencia y Protocolo Adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (2001);

Consejo de Europa, Convenio para la protección de los niños contra la explotación y el abuso sexual (2007);

Comunidad Económica de los Estados de África Occidental (CEDEAO), proyecto de directiva sobre la lucha contra la ciberdelincuencia en la CEDEAO (2009);

Liga de los Estados Árabes, Convention on Information Technology Offences (2010);

Organización de Cooperación de Shanghái, Acuerdo Intergubernamental sobre Cooperación en el Ámbito de la Seguridad de la Información a Nivel Internacional (2010)

Mercado Común para África Oriental y Meridional (COMESA);

Proyecto de ley modelo sobre la ciberseguridad (2011);

Unión Africana, proyecto de convención sobre el establecimiento de un marco jurídico propicio a la seguridad cibernética en África (2012);

Unión Europea, decisión marco 2001/413/JAI del Consejo sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo (2001);

Unión Europea, decisión marco 2005/222/JAI del Consejo sobre los ataques contra los sistemas de información (2005);

Unión Europea, documento COM (2010) 517 final, Propuesta de directiva Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo (2010).

32. Los principales métodos utilizados para intercambiar pruebas electrónicas son los de la cooperación tradicional, tales como solicitudes oficiales de asistencia judicial recíproca. Hay una serie de acuerdos bilaterales, regionales e internacionales relativos a los procedimientos de asistencia judicial recíproca. Muchos de los instrumentos regionales e internacionales sobre la ciberdelincuencia enumerados anteriormente contienen disposiciones sobre esa asistencia. Los procedimientos y solicitudes de asistencia judicial recíproca se fijan principalmente en acuerdos regionales y bilaterales. Entre los ejemplos de acuerdos

regionales sobre asistencia judicial recíproca cabe citar el Tratado sobre asistencia judicial recíproca en asuntos penales de la Asociación de Naciones de Asia Sudoriental (ASEAN), de 2004, y el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea del Consejo de Europa, de 2000.

33. En vista del carácter a menudo volátil y fácilmente contaminable de las pruebas electrónicas, es posible que las respuestas necesarias para obtenerlas no siempre se proporcionen oportunamente a través de los mecanismos oficiales de cooperación. Así, también pueden utilizarse mecanismos de cooperación oficiosa y las redes accesibles de manera ininterrumpida, en particular, ofrecen grandes posibilidades de racionalizar esa cooperación o incluso facilitar, en una etapa posterior, la cooperación oficial. No obstante, la diligencias investigativas que la cooperación oficiosa permite llevar a cabo pueden variar considerablemente. Un obstáculo que plantea al intercambio oficioso de pruebas electrónicas es que muchos países prohíben el uso de pruebas obtenidas a través de mecanismos no oficiales en el contexto de procedimientos judiciales[21].

34. A la hora de aportar información para el estudio sobre el delito cibernético, los países que hacen uso de la cooperación oficiosa señalaron que los mecanismos pertinentes dependían de la existencia de entidades homólogas competentes y bien organizadas en el extranjero y que ello era más probable cuando la cooperación informal en materia de aplicación de la ley se regía por algún tipo de acuerdo. Varios países observaron que la cooperación oficiosa se llevaba pues a cabo sobre la base de acuerdos regionales y bilaterales utilizando las redes establecidas por organizaciones e instituciones internacionales y regionales; con la asistencia de las embajadas y los consulados; y a través de redes privadas de funcionarios encargados del cumplimiento de la ley.

35. Con ese objetivo, el artículo 27 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional contiene disposiciones sobre cooperación en materia de cumplimiento de la ley y en ella se alienta a los Estados a considerar la posibilidad de celebrar acuerdos o arreglos bilaterales o multilaterales que permitan la cooperación entre diferentes órganos encargados de hacer cumplir la ley. Por otra parte, los Estados también han promulgado varias leyes sobre cooperación en materia de cumplimiento de la ley, en particular por lo que se refiere, entre otras cosas, al intercambio de información, las investigaciones conjuntas y la vigilancia electrónica o de otra índole.

36. Si bien algunos países recurren a la cooperación entre servicios policiales, otros se centran principalmente en la cooperación oficiosa por conducto de la INTERPOL. La INTERPOL tiene oficinas en 190 países, las cuales a menudo están vinculadas a los órganos de orden público[22]. En consecuencia, las oficinas pueden apoyar las relaciones informales, lo que aumenta la posibilidad de encontrar alternativas a los procedimientos oficiales de cooperación internacional.

---

[21] *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, capítulo 4, pág. 47 (véase *infra*), disponible en www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf.

[22] Estudio sobre el delito cibernético, capítulo 7, pág. 187.

37. Diversos problemas relacionados con los procedimientos de cooperación oficiales y oficiosos respecto de las pruebas electrónicas en los asuntos penales pueden obstaculizar la recopilación y el intercambio de dichas pruebas. Ejemplos de ello son las diferencias entre el alcance de las disposiciones sobre cooperación de los instrumentos multilaterales y bilaterales, la falta de plazos obligatorios de respuesta, la multiplicidad de redes oficiosas de aplicación de la ley y las diferencias entre las salvaguardias en materia de cooperación[23].

III. Instrumentos elaborados por la Oficina de las Naciones Unidas contra la Droga y el Delito

38. En los últimos años, la UNODC ha elaborado una serie de instrumentos que permiten abordar la cuestión de las pruebas electrónicas a partir de diferentes perspectivas, disciplinas y mandatos. Esos instrumentos abarcan un espectro de conocimientos que se refuerzan mutuamente, los cuales se reúnen a menudo a través de amplias consultas con los Estados Miembros y las partes interesadas. Los instrumentos de la UNODC, que van desde análisis basados en la investigación acerca de determinados tipos de delitos hasta plataformas que proporcionan acceso directo a recursos jurídicos, ofrecen una combinación polifacética de fuentes de conocimientos sobre la reunión y el intercambio de pruebas electrónicas.

39. Si bien no se ha dedicado ningún instrumento de la UNODC exclusivamente a las pruebas electrónicas, la Oficina cuenta con una serie de materiales e instrumentos de orientación e investigación que son pertinentes al tema que se examina, los cuales se presentan a continuación.

A. Estudios preparados por la Oficina de las Naciones Unidas contra la Droga y el Delito en cumplimiento de resoluciones de las Naciones Unidas

40. De conformidad con los mandatos pertinentes del Consejo Económico y Social, en los últimos años la Oficina de las Naciones Unidas contra la Droga y el Delito ha publicado los estudios siguientes, que se refieren, entre otras cosas, a la reunión y el intercambio de pruebas electrónicas en el contexto de determinados tipos de delitos: a) el Manual sobre los delitos relacionados con la identidad[24]; y b) el estudio sobre la incidencia de las nuevas tecnologías de la información en el abuso y la explotación de niños[25] (en adelante, “estudio sobre el abuso y la explotación de niños”).

41. Análogamente, con arreglo a las resoluciones 65/230 y 67/189 de la Asamblea General, la UNODC prestó apoyo técnico y de secretaría a las reuniones del grupo intergubernamental de expertos de composición abierta encargado de realizar un estudio exhaustivo del problema del delito cibernético. En ese contexto, la UNODC preparó un proyecto de estudio exhaustivo del problema del delito

---

[23] Estudio sobre el delito cibernético, capítulo 7, págs. 197 a 215.

[24] www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf.

[25] Véase la nota 21.

cibernético sobre la base de la información proporcionada por los Estados miembros, que se cita como referencia en diferentes partes de este documento de antecedentes.

1. Manual sobre los delitos relacionados con la identidad

42. El Manual, publicado por la UNODC en 2011 en cumplimiento de las resoluciones 2007/20 y 2009/22 del Consejo Económico y Social sobre la cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude económico y los delitos relacionados con la identidad, se centra en determinadas cuestiones jurídicas y políticas del relativas al delito de identidad, entre las que figuran la reunión y el uso de información y datos electrónicos. Su principal objetivo es exponer diversas opciones y consideraciones que deben tenerse en cuenta al abordar cuestiones de justicia penal internas (como la tipología de los delitos, los diferentes criterios para su tipificación y la protección de las víctimas), los problemas concretos que se presentan en el ámbito de la cooperación internacional en materia penal y la posibilidad de crear sinergias y alianzas entre los sectores público y privado, sobre todo en la esfera de la prevención de los delitos relacionados con la identidad. Los documentos de investigación junto con el material práctico que forma parte del Manual contribuyen a esclarecer los diferentes aspectos y parámetros de los complejos problemas que plantea esta forma de delincuencia.

43. Dada la variedad de los temas abarcados, el Manual está destinado a los legisladores, los responsables de formular políticas, los fiscales, las autoridades encargadas de hacer cumplir la ley, los profesionales de servicios pertinentes, así como otros interesados (representantes de las organizaciones internacionales e intergubernamentales competentes, del sector privado y los círculos académicos).

44. El Manual también puede servir de referencia en los programas de asistencia técnica y las actividades de fomento de la capacidad encaminadas a ampliar los conocimientos especializados para abordar las cuestiones de carácter jurídico, institucional y operacional relacionadas con los delitos de identidad como nueva forma de delincuencia.

45. Además, la guía práctica relativa a la cooperación internacional para combatir los delitos relacionados con la identidad, contenida en el Manual sobre los delitos relacionados con la identidad, incluye una sinopsis de los aspectos relativos a la dimensión transnacional de los delitos relacionados con la identidad y se centra en la información básica y las directrices sobre cómo tratar mejor las solicitudes de cooperación internacional en este ámbito, entre otras cosas presentando ejemplos de los casos más pertinentes.

2. Estudio sobre la incidencia de las nuevas tecnologías de la información en el abuso y la explotación de niños

46. En respuesta a la resolución 2011/33 del Consejo Económico y Social, titulada “Prevención, protección y cooperación internacional contra el uso de las nuevas tecnologías de la información para el abuso y/o explotación de los niños”, en 2015 la UNODC publicó un estudio sobre los efectos de las nuevas tecnologías de la información en el abuso y la explotación de niños (que fue presentado inicialmente en el 23° período de sesiones de la Comisión de Prevención del Delito

y Justicia Penal, celebrado en mayo de 2014). El estudio se basa en investigaciones de fuente abierta sobre la cuestión y la labor de la reunión oficiosa de expertos de la UNODC sobre el tema, que tuvo lugar en Viena del 23 al 25 de septiembre de 2013 y contó con la participación de expertos de organizaciones internacionales, organismos encargados de hacer cumplir la ley, otros profesionales competentes y miembros del mundo académico. El estudio proporciona información básica pertinente sobre los temas siguientes:

a) términos y definiciones nuevos;

b) la tipología de los delitos;

c) los tipos más comunes y las formas de comportamiento relacionadas con ellos;

d) las principales formas de tecnologías de la información y las comunicaciones que facilitan determinados tipos de delitos, como el abuso y la explotación de niños;

e) el perfil y la competencia tecnológica del delincuente;

f) los factores de riesgo de victimización;

g) la naturaleza de materiales como fotografías, negativos, diapositivas, revistas, libros, dibujos, películas, cintas de vídeo y discos o archivos informáticos; y

h) los tipos de dispositivos y plataformas que se utilizan con fines delictivos, tales como: teléfonos móviles, servicios de almacenamiento remoto con tecnología de cifrado incorporada, computación en nube y nuevas aplicaciones, como Snap Chat y Wickr, que permitan a los usuarios distribuir imágenes temporales que desaparecen en cuestión de segundos después de la recepción.

47. Por otra parte, el capítulo III del estudio está dedicado a la investigación del abuso y la explotación de niños basados en el uso de la tecnología de la información y las comunicaciones.

48. En el estudio se analiza la accesibilidad y la aplicación práctica de programas informáticos y tecnologías relacionados con imágenes que permiten a los organismos de policía identificar y rescatar a víctimas no identificadas que aparecen en materiales en línea y organizar sus investigaciones forenses comparando los materiales digitales de los sospechosos con las imágenes digitales disponibles en bases de datos. El estudio proporciona información útil sobre las tecnologías innovadoras que se utilizan para reducir la duplicación de labores investigativas y, al mismo tiempo, obrar en interés de la protección de las víctimas. Tal es el caso, por ejemplo, de las siguientes:

El programa “PhotoDNA” de Microsoft: se trata de un programa informático gratuito que se utiliza para crear una firma singular, parecida a una impresión digital, para una imagen digital, que puede compararse con la firma de otras imágenes a fin de encontrar duplicados de esa imagen;

Las bases de datos de imágenes de abusos que incluyen información sobre víctimas identificadas y no identificadas[26], y

La base internacional de datos de imágenes de explotación sexual de niños de la INTERPOL: se trata de una base de datos que se emplea para identificar y rescatar a víctimas no identificadas utilizando complejos programas informáticos de comparación de imágenes para establecer relaciones entre víctimas y lugares.

49. Las innovaciones técnicas mencionadas anteriormente son utilizadas también por los proveedores de servicios de Internet para encontrar y eliminar algorítmicamente de sus servidores el material de abuso sexual de niños.

50. Por otra parte, el análisis forense digital se describe en el estudio como la rama de la ciencia forense que se ocupa de la recuperación y la investigación de huellas digitales generadas por computadora. A este respecto, el estudio pone de relieve los tipos de datos informáticos y comunicaciones electrónicas que podrían ser pertinentes en relación con un acto delictivo, la variedad de formatos y sistemas que pueden utilizarse para archivarlos y los instrumentos empleados para examinar los datos.

51. El estudio también se refiere a la utilización de programas informáticos de “búsqueda automatizada” en las investigaciones forenses y destaca el uso de este instrumento para encontrar con facilidad y rapidez sitios y contenidos etiquetados con palabras clave de uso común.

52. Asimismo, analiza los avances emprendidos durante el último decenio en el desarrollo y despliegue de instrumentos de tecnología y programas informáticos que permiten la búsqueda rápida de datos pertinentes en miles de bases de datos, registros financieros, muestras de ADN, muestras de sonido, videoclips, mapas, planos, informes de agentes de inteligencia y redes sociales diferentes. Esos instrumentos entrelazan los datos pertinentes poniendo de relieve una ruta precisa, coherente y útil y proporcionan análisis conceptuales de enlaces.

53. Además, el estudio examina la conveniencia y las características específicas de la labor de investigación de los agentes infiltrados con respecto a la delincuencia en línea.

3. Proyecto de estudio exhaustivo sobre el delito cibernético

54. En el capítulo 6 del proyecto de estudio exhaustivo sobre la ciberdelincuencia se analiza el tema de las pruebas electrónicas y la justicia penal a partir de la necesidad de determinar, reunir y analizar las pruebas electrónicas mediante el análisis forense digital. En él se examinan la admisibilidad y el uso de pruebas electrónicas en los procesos penales y se demuestra que una serie de dificultades procesales pueden influir en el funcionamiento del sistema de justicia penal.

[26] Tales como las bases de datos creadas por la INTERPOL y el National Centre for Missing and Exploited Children (NCMEC) de los Estados Unidos.

Se establece un vínculo entre las necesidades en materia de aplicación de la ley y justicia penal y las actividades de asistencia técnica ejecutadas y necesarias.

55. Además, algunos aspectos relacionados con las pruebas electrónicas se examinan desde el punto de vista del alcance de la cooperación para hacer cumplir la ley y la cooperación internacional. En este sentido, el capítulo 5 (relativo a la aplicación de la ley y las investigaciones) trata del examen, la utilización, el almacenamiento, la retención y la conservación de datos electrónicos que pueden presentarse como pruebas electrónicas; la recopilación de datos en tiempo real; las herramientas de análisis forense a distancia; el acceso directo de los órganos de orden público a datos extraterritoriales; los derechos humanos y las investigaciones policiales y la obtención de datos de proveedores de servicios del sector privado. Por otra parte, el capítulo 7 (relativo a la cooperación internacional) hace referencia al tema de las pruebas extraterritoriales obtenidas de proveedores de servicios y nubes y trata en detalle asuntos como la ubicación de datos; el acceso extraterritorial a datos durante la reunión de pruebas; y la obtención de datos de proveedores de servicios extraterritoriales.

B. Instrumentos elaborados por la Oficina de las Naciones Unidas contra la Droga y el Delito para su utilización en el contexto de las actividades de asistencia técnica

56. Los programas de asistencia técnica de la UNODC han permitido elaborar instrumentos prácticos para abordar el tema de las pruebas digitales desde la óptica de un profesional. A este respecto, los participantes en la segunda reunión interregional sobre el intercambio de prácticas de solicitud y suministro de pruebas digitales en la investigación de delitos de delincuencia organizada y el enjuiciamiento de los responsables[27] formularon una serie de consejos básicos dirigidos a investigadores y fiscales para solicitar pruebas y datos electrónicos y digitales a jurisdicciones extranjeras.

57. Se trata de consejos prácticos para solicitar pruebas electrónicas a jurisdicciones extranjeras, incluidos consejos para la obtención de pruebas electrónicas procedentes de fuentes de acceso público o directamente de proveedores de servicios de Internet establecidos o registrados en el país requirente como filiales de proveedores de esos servicios con sede en el extranjero; la conservación de pruebas electrónicas antes del envío de la solicitud de divulgación; el envío, siempre que sea posible, de la solicitud directamente al proveedor de servicios de Internet, con copia al órgano de investigación o fiscal del país requerido; y las consultas sobre los aspectos técnicos de la solicitud con la dependencia de delitos cibernéticos.

58. En cumplimiento de la resolución 7/4 de la Conferencia de las Partes en la Convención contra la Delincuencia Organizada, la UNODC sigue elaborando instrumentos de cooperación internacional, en particular el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca. A este respecto, la UNODC ha

[27] Tbilisi (Georgia), 9 a 11 de diciembre de 2014. Este instrumento se elaboró como parte de la iniciativa de la UNDOC para establecer y reforzar la red de fiscales y autoridades centrales de los países de origen, tránsito y destino en respuesta a la delincuencia organizada transnacional en Asia Central y el Cáucaso meridional.

organizado una serie de reuniones oficiosas de grupos de expertos para examinar y debatir la reelaboración de este instrumento y examinar orientaciones sobre su uso en el futuro.

59. Durante la última de esas reuniones, celebrada en mayo de 2015, los participantes acordaron la inclusión en el instrumento reelaborado de un módulo sobre pruebas electrónicas que pudiera ayudar a los Estados a solicitar asistencia en relación con ese tipo de pruebas. A este respecto, los expertos compartieron experiencias nacionales en cuanto a solicitar y obtener pruebas digitales, incluso por lo que se refería al grado de disponibilidad de plantillas para pruebas digitales y a si existían criterios normalizados de descripción de dichas pruebas. La reunión proporcionó orientación sobre el formato y la estructura posibles del módulo sobre pruebas digitales haciendo hincapié en los distintos tipos de pruebas digitales, como datos de equipo, datos de red, información sobre suscriptores y datos de contenido. Se esperaba ultimar la versión reelaborada del Programa como resultado de otra reunión oficiosa de expertos que se celebraría los días 22 y 23 de octubre de 2015 en Viena.

C. Plataformas de gestión de conocimientos de la Oficina de las Naciones Unidas contra la Droga y el Delito

1. Portal de gestión de conocimientos para el intercambio de recursos electrónicos y legislación sobre delincuencia (portal SHERLOC)

60. La UNODC ha seguido dedicándose al desarrollo del portal SHERLOC de gestión de conocimientos para el intercambio de recursos jurídicos relativos a la delincuencia. La atención se ha centrado en la recopilación de recursos relativos a diferentes tipos de delitos y temas conexos, entre ellos el de las pruebas electrónicas. Al 18 de agosto de 2015, el portal contenía 44 leyes pertinentes que establecen normas sobre la prueba electrónica.

2. Archivo de datos sobre el delito cibernético

61. Además del portal SHERLOC, la UNODC ha creado un archivo de datos sobre el delito cibernético, que consta de una base de datos central de leyes y lecciones aprendidas cuyo fin es facilitar la evaluación continua de las necesidades y la capacidad de los organismos policiales y judiciales y la prestación de asistencia técnica y su coordinación.

62. El archivo, que entró en funcionamiento en 2015 y se basa en la información proporcionada y actualizada por los Estados Miembros, es el primer instrumento mundial de acceso a leyes, jurisprudencia y lecciones aprendidas sobre el delito cibernético y las pruebas electrónicas. El archivo tiene múltiples objetivos, entre ellos los de: permitir a los legisladores recurrir a la base de datos de legislación a la hora de redactar leyes sobre el delito cibernético o las pruebas electrónicas; facilitar la cooperación internacional ayudando a las fuerzas del orden y a los fiscales a determinar qué disposiciones legislativas son aplicables a la delincuencia cibernética en otros Estados Miembros; y proporcionar a los usuarios ejemplos de buenas prácticas de prevención, investigación y enjuiciamiento de delitos cibernéticos. La legislación nacional sobre la asistencia judicial recíproca no siempre menciona o establece las funciones de la autoridad central. Cuando lo hace,

puede designar una institución gubernamental como autoridad central, proporcionar una lista de sus funciones y, en algunos casos, contener una cláusula de salvaguardia que confirme que la ley no limita la facultad de la autoridad de formular o recibir solicitudes o de cooperar con un Estado extranjero por otras vías o medios. A título de ejemplo, la ley sobre asistencia jurídica de un país europeo especifica que la autoridad central: "1) recibirá las solicitudes de asistencia …; 2) dará cumplimiento, ya sea directamente o por conducto de [otras] autoridades, a las solicitudes ...; 3) transmitirá las solicitudes de asistencia; y 4) traducirá los documentos".

IV. Conclusiones y recomendaciones

63. El Grupo de Trabajo sobre Cooperación Internacional tal vez desee recomendar a la Conferencia de las Partes que:

a) pida a la Secretaría que preparare, en cooperación con las organizaciones intergubernamentales pertinentes y con sujeción a la disponibilidad de fondos extrapresupuestarios, un manual de reunión e intercambio de pruebas electrónicas;

b) pida a la Secretaría que, como parte de sus esfuerzos por mejorar los instrumentos de cooperación internacional, incorpore el tema de la prueba electrónica;

c) solicite a los Estados Miembros que notifiquen a la Secretaría la existencia de estructuras o dependencias especializadas en la lucha contra el delito cibernético para su inclusión en el Directorio de Autoridades Nacionales Competentes.