MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

PRIMERA REUNION DE CiberRed/CiberRede

5 de febrero de 2018

Conclusiones de la Coordinación

ÍNDICE

PRIMERA REUNIÓN DE CiberRed/*CiberRede*

CONCLUSIONES DE LA COORDINACIÓN

1. Se celebró el 5 de febrero de 2018, en Lisboa, en la Procuraduría-General de la República de Portugal, la primera reunión del CiberRed/*CiberRede*, la red iberoamericana de fiscales especializados en ciberdelito.

Participaron en la reunión representantes de 18 de los países de la AIAMP[1], apenas no habiendo estado representados Ecuador, Nicaragua y Venezuela. Se adjunta, como Anexo A, la lista de participantes.

2. CiberRed/*CiberRede* se estableció por resolución de la XXIV Asamblea General de la Asociación Iberoamericana de Ministerios Públicos - AIAMP (celebrada en Lisboa en octubre de 2016). Se trata de una red de procuradores / fiscales especializados en ciberdelito, que tiene el objetivo de promover y mejorar la información disponible sobre los diferentes sistemas jurídicos iberoamericanos en el ámbito de la ciberdelincuencia, potenciar el intercambio de experiencias y conocimientos necesarios para solucionar los múltiples problemas que se plantean en esta área, crear y difundir buenas prácticas entre sus integrantes y optimizar y agilizar la cooperación institucional y las solicitudes de cooperación judicial internacional entre los distintos países.

Además, en la XXIV Asamblea General de la AIAMP se deliberó que esta red sería un foro de contacto e intercambio sobre las tendencias de la ciberdelincuencia y la obtención de pruebas digitales y, a tal fin, debería celebrar una reunión anual de los puntos de contacto.

3. Este fue el contexto de la realización de la primera reunión de CiberRed/*CiberRede*, para la cual se definió, como temática estratégica, el "*ciberdelito en el espacio iberoamericano - fenómenos criminales y legislación*". Se adjunta, como Anexo B, la agenda de la reunión.

4. Se describen de seguida las conclusiones que la Coordinación de la red, asegurada por Portugal, extrajo de la reunión.

---

[1] Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, El Salvador, España, Guatemala, Honduras, México, Panamá, Paraguay, Perú, Portugal, República Dominicana y Uruguay

5. Una de las conclusiones más visibles de la reunión dice respecto a la existencia de marcos normativos en materia de ciberdelito en los países del espacio iberoamericano. A este propósito, resultó de la reunión que muchos de los países tienen ya marcos normativos específicos a este respecto (sea llamándolos de crímenes informáticos, crímenes cibernéticos, ciberdelitos o cibercrimenes).
Sin embargo, así no sucede con un número aún significativo de países, que sólo tienen previsiones legales de crímenes más genéricos, aunque susceptibles de ser practicados en las redes. No siempre estos últimos se adaptan a las nuevas realidades, por lo que es necesaria alguna innovación legislativa o, al menos, algún ajuste legal. En la mayoría de estos casos, existe la necesidad de introducir legislación en materia de delitos informáticos o ciberdelitos, propiamente dichos. Algunos de estos últimos países ya están dando pasos en este sentido, inspirándose tanto en el Convenio de Budapest, como en las legislaciones de otros países del grupo.

6. La conclusión es más pesimista en lo que se refiere a las normas relativas a la obtención de pruebas digitales: sólo un pequeño número de países iberoamericanos tiene normas de procedimiento específicamente dirigidas a la obtención de pruebas digitales. En algunos casos, los marcos normativos generales se están aplicando al entorno digital, aunque con insuficiencia.
A este respecto, además de la carencia normativa, se identificó también la necesidad de una discusión más detallada, con respecto a la definición de las lagunas de cada uno de los países.

7. Se adjuntan, como Anexo C, súmulas de los cuadros normativos de los distintos países presentes en la reunión.

8. En otro aspecto, fue posible concluir que, de modo uniforme en los distintos países, los crímenes en las redes de comunicaciones están en gran expansión. Por su complejidad, requieren

conocimientos especializados y medios específicos de investigación. Se aclaró la necesidad generalizada de formación de magistrados, así como su especialización. También fue recurrentemente afirmada la necesidad de actualización frecuente de dicha formación, sea por medio del intercambio de conocimientos y buenas prácticas entre procuradores/fiscales, sea por medio de debate de casos prácticos.

9. Fue también una de las claras conclusiones, la necesidad de especialización de procuradores/fiscales en esta área. Esta especialización, ya existente en algunos de los países iberoamericanos, fue insistentemente afirmada con una necesidad inevitable, al no ser posible investigar ciberdelito de otra forma.

10. Finalmente, aún se han podido extraer de las discusiones dos conclusiones sobre la misma CiberRed/*CiberRede* y su funcionamiento.
De un lado, se concluye que habría ventaja en la utilización, por los puntos de contacto de la red, de la ya existente plataforma *Iber@*, gestionada por IberRed. El uso de dicha plataforma permitirá a los puntos de contacto de CiberRed/*CiberRede* comunicarse con seguridad, siendo también un vehículo de impulso de la red.
Por otro lado, también se ha señalado las claras ventajas de mantener este tipo de reuniones com regularidad. Como temas importantes a discutir, en reuniones futuras, se avanzó la obtención de datos de operadores de comunicaciones, sobre todo extranjeros, y las distintas posibilidades de cooperación informal en la obtención de prueba digital.

23 de marzo de 2018

ANEXO A

Primera Reunión Anual de CiberRed/*CiberRede*

LISTA DE PARTICIPANTES

País / *País*	Nome / Nombre	Cargo / Función
ARGENTINA	**Horacio Azzolín**	Unidad Especializada en Ciberdelincuencia
BOLIVIA	**Javier Flores Mamani**	Fiscal de Materia
BRASIL	**Carlos Bruno Ferreira da Silva**	*Gabinete de Relações Internacionais do Ministério Público Federal*
BRASIL	**Neide de Oliveira**	*Coordenadora do Grupo de Trabalho sobre Crimes Cibernéticos*
CHILE	**Mauricio Fernández Montalbán**	Director-Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (Fiscalía Nacional)
COLOMBIA	**Luis Orlando Paloma Parra**	Fiscal del eje de cibercriminalidad de la Dirección contra las organizaciones criminales
COSTA RICA	**Elvis Antonio López Matarrita**	Fiscal
CUBA	**Dimas Herrera Gandol**	Secretaria del Fiscal General
EL SALVADOR	**Duglas Gilberto Espinal Claros**	Jefe de la Unidad de Análisis de Información Fiscal
ESPAÑA	**Elvira Tejada**	Fiscal de Sala de Criminalidad Informática
ESPAÑA	**Ana Maria Martín**	Fiscal de Criminalidad Informática
GUATEMALA	**María Elena Galvez Rafael**	Jefa del Departamento de Ciber Delito
HONDURAS	**Marisol Rodriguez**	Fiscal Jefe de la Fiscalía Especial de la Niñez
MÉXICO	**Marco Mecalco Raya**	Unidad de Investigaciones Cibernéticas
PANAMÁ	**Lizeth Girón**	Fiscal
PARAGUAY	**María Soledad Machuca Vidal**	Fiscal Adjunta encargada de la Unidad Especializada de Delitos Informáticos del Ministerio Público
PERÚ	**Alonso Raúl Peña Cabrera Freyre**	Fiscal Superior Jefe de la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación
PORTUGAL	**Pedro Verdelho**	*Coordenador do Gabinete Cibercrime*
PORTUGAL	**Maria de Lurdes Lopes**	*Assessora do Gabinete da Procuradora-Geral da República*
PORTUGAL	**Raul Farias**	*Assessor do Gabinete da Procuradora-Geral da República*
REPÚBLICA DOMINICANA	**John Henry Reynoso Ramírez**	Procurador General de Corte, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología
URUGUAY	**Enrique Rodríguez**	Fiscal Letrado Penal de Montevideo de Delitos económicos y complejos

COUNCIL OF EUROPE	**Manuel de Almeida Pereira**	*Project Manager* *Cybercrime Programme Office (C-PROC)*
COUNCIL OF EUROPE	**Oana Tarus**	*Project Assistant* *Cybercrime Programme Office (C-PROC)*
COUNCIL OF EUROPE EXPERT	**Rodolfo Orjales**	*Federal Prosecutor - USA*
COUNCIL OF EUROPE EXPERT	**Marcos Salt**	Coordinador del Programa Nacional contra la Criminalidad Informática - Argentina

ANEXO B

1ª Reunião Anual da CiberRede **REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME**	***1ª Reunión Anual de CiberRed*** ***RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA***
Lisboa, 5 de Fevereiro de 2018	***Lisboa, 5 de Febrero de 2018***

AGENDA
5 Fevereiro de 2018 / 5 Febrero de 2018

10:00	Abertura
10:15	A realidade do cibercrime no espaço IberoAmericano (fenómenos criminais e legislação) – intercâmbio de experiências entre os pontos de contacto e outros representantes nacionais (discussão entre os participantes)
11:15	**Pausa**
11:30	Plataforma Iber@: sua possível utilização pela CiberRede, - Ana Martin, *fiscal especializada* em
11:45	cibercrime, Espanha) Objetivos estratégicos da *CiberRede* para o próximo triénio; próxima reunião da *CiberRede* - tema e formato – discussão entre os participantes
12:30	Conclusões e encerramento

10:00	*Inauguración*
10:15	*La realidad del ciberdelito en el espacio iberoamericano (los fenómenos criminales y la legislación) - intercambio de experiencias entre los puntos de contacto y otros representantes nacionales (discusión entre los participantes)*
11:15	***Pausa***
11:30	*Plataforma Iber@: su posible utilización por CiberRed, Ana Martin, fiscal especializada en criminalidad informática, España;)*
11:45	*Objetivos estratégicos de CiberRed para el próximo trienio; próxima reunión de CiberRed - tema y formato (discusión entre los participantes) Conclusiones y*
12:30	*cierre*

ANEXO C

CIBERDELITO Y PRUEBA DIGITAL

SÚMULAS DE LOS MARCOS NORMATIVOS

	NORMAS EN VIGOR	PROYECTOS LEGISLATIVOS
ARGENTINA	El Código Penal, por medio de la Ley 26388 (http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm) y de la Ley 26904 (http: //servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm) incluye la mayoría de los tipos de delitos del Convenio de Budapest. No existen normas específicas sobre prueba digital, ya que el Código Procesal Penal, modificado por la Ley 27063 (http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/norma.htm#28), sólo incluye, en los artículos 143 y 144, la interceptación de comunicaciones y la incautación de datos.	Hay un proyecto de modificación del Código Penal, para pasar a incluir nuevas conductas (como por ejemplo la *revenge porn*). Hay planes para ajustar el Código Procesal Penal.
BOLIVIA	No existen tipos específicos de crímenes en este campo - sólo, en el Código Penal, un crimen de manipulación informática de datos y de alteración, acceso y uso indebido de datos. No existen normas específicas sobre la prueba digital - se aplican, dentro de lo posible, las normas generales.	
BRASIL	La Ley 12737 (https://www.jusbrasil.com.br/topicos/10605134/artigo-266-del-decreto-el-n-2848-de-24-de-feema-de-1891) introdujo en el Código Penal (Artículos 154 bis, 154-B, 266 y 313 bis) los delitos de acceso ilegítimo, difusión ilícita de dispositivos y ataques de denegación de servicio. Todavía criminalizó la falsificación de tarjetas de crédito. El Estatuto de la Niñez y el Adolescente (https://presrepublica.jusbrasil.com.br/legislacao/91764/estatuto-de-crianca-eldo-adolescente-el-8069-90#art-240), en los artículos 240, 241-A, 241-B, 241-C y 241 E, prevé la incriminación de la pornografía infantil. No existen normas específicas sobre la prueba digital.	En el Senado se está pendiente el Proyecto de Ley PL 236/2012 (proyecto de nuevo Código Penal), que prevé los crímenes del Convenio de Budapest (https://www25.senado.leg.br/web/atividad/materias/-/materia/106404/pdf).
CHILE	La Ley N.º 19.223, de 1993 (http://bcn.cl/1uw5c), tipifica figuras penales relativas a la informática. El Código de Proceso Penal tiene algunas normas aplicables a la obtención de prueba digital (en los	Actualmente está en discusión un proyecto de ley de modificación del cuadro sustantivo (Boletín N.º 10145-07 -

	Artículos 222 a 226 bis), en particular sobre interceptación de comunicaciones.	http://www.senado.cl/appsenado/templates/tramitacion/index.php)
COLOMBIA	El Código Penal (modificado por la Ley 1273, de 2009), incluye ciberdelitos. No existen normas específicas sobre prueba digital.	
COSTA RICA	Hay una sección específica en el Código Penal que incluye delitos informáticos y conexos. No hay normas de procedimiento específicas a este propósito, pero el principio de libertad probatoria permite la obtención de prueba digital - con límites en el acceso a cierto tipo de prueba, como por ejemplo la interceptación de comunicaciones.	
CUBA	No existen tipos específicos de delitos en este ámbito. No existen normas específicas sobre la prueba digital.	Están en fase de estudio, aún no público, nuevos códigos Penal y de Proceso Penal que incluirán aspectos relacionados con las tecnologías
EL SALVADOR	La Ley Especial contra Delitos Informáticos y Conexos (Decreto 260, de 2016) incluye muchos tipos de ilícitos - y también todos los previstos en el Convenio de Budapest. En el Código Procesal Penal (Decreto 733 de 2009) y en leyes especiales hay disposiciones relativas a la prueba: Decreto 953, de 2015 (ley especial contra la extorsión), Decreto 108, de 2006 (terrorismo) y Ley Especial para las Intercepciones Telefónicas.	
ESPAÑA	El Código Penal Español transpone las normas penales sustantivas previstas del Convenio de Budapest. La Ley de Enjuiciamiento Criminal, tras la modificación de la LO 13/2015, de 5 de octubre, a su vez, transpone las normas procesales del Convenio.	Está pendiente en el parlamento una propuesta legislativa de incriminación de la suplantación de identidad.
GUATEMALA	No existen todavía tipos específicos de crímenes en este campo. También no existen normas específicas sobre la prueba digital.	Existe un proyecto legislativo con el propósito específico de transponer el Convenio de Budapest, en una de las comisiones especializadas del Congreso.
HONDURAS	No existen específicos crímenes en este campo en el Código Penal - sólo delitos relativos a la seguridad de las redes. No existen normas específicas sobre la prueba digital.	
MÉXICO		Está en discusión en el gobierno la introducción de un Código

	Existe un Código Penal Federal y varios Códigos Penales de los Estados, que incluyen normas en el ámbito de la ciberdelincuencia. A pesar de que existe un único Código Procesal Penal a nivel nacional, no existen normas específicas sobre la prueba digital.	Penal Nacional único, siendo propósito que incluya un capítulo sobre ciberdelitos.
PANAMÁ	Todavía no hay un cuerpo consolidado de tipos específicos. No existen normas específicas sobre la prueba digital.	Existe un proyecto legislativo que pretende adecuar la legislación nacional al Convenio de Budapest. Fue introducida en el Congreso en 2017.
PARAGUAY	La ley de 2011 consagra ya algunas normas penales de acuerdo con el Convenio de Budapest. No existen normas específicas sobre la prueba digital.	
PERÚ	La ley interna (Ley 80086) cubre todas las normas sustantivas del Convenio de Budapest y, así mismo, todas sus normas procesales.	
PORTUGAL	La Ley del Ciberdelito (Ley 109/2009) transpone todas las normas del Convenio de Budapest - sustantivas, procesales y de cooperación internacional.	
REPÚBLICA DOMINICANA	La ley interna transpone todas las normas sustantivas y de procedimiento del Convenio de Budapest.	Está en análisis en el Congreso, en sede de comisión especializada, un proyecto de modernización de la ley vigente.
URUGUAY	No hay tipos específicos de crímenes en este campo. No existen en la ley normas específicas sobre prueba digital - sólo se prevé, en términos generales, en el Código de Proceso Penal, la interceptación de comunicaciones.	Hay un proyecto legislativo que introducirá algunos de los crímenes descritos en el Convenio de Budapest (acceso no autorizado, daño informático y estafa informática). Este proyecto está aún en fase de aprobación por el poder ejecutivo y sólo después se remitirá al Congreso.