CONFERÊNCIA INTERNACIONAL

e

SEGUNDA REUNIÃO da

CiberRede/*CiberRed*

(25 e 26 de junho de 2019)

CONCLUSÕES DA COORDENACÃO

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

AIAMP
Asociación Ibero Americana de Ministerios Públicos

CONFERÊNCIA INTERNACIONAL E SEGUNDA REUNIÃO DA CiberRede/*CiberRed*

CONCLUSÕES DA COORDENAÇÃO

A – A REUNIÃO

1. Decorreu, a 26 de junho de 2019, em Santiago, Chile, a segunda reunião da CiberRede/*CiberRed*, a Rede Ibero-Americana de Ministérios Públicos Especializados em Cibercrime. Conjugadamente, com ela, a 25 e 26, decorreu uma conferência internacional sobre cibercriminalidade e obtenção de prova digital, dirigida aos pontos de contacto da rede. Estiveram presentes 27 participantes, que representaram 15 países da AIAMP[1], apenas não tendo estado representados as Honduras, El Salvador, o Equador, a Nicarágua, o Uruguai[2] e a Venezuela. Junta-se, como Anexo A, a lista de participantes e como Anexo B a agenda das reuniões.

2. A CiberRede/*CiberRed* foi constituída por deliberação da XXIV Assembleia Geral da Associação Ibero-Americana de Ministérios Públicos – AIAMP (realizada em Lisboa, em outubro de 2016). Conta, presentemente, com pontos de contacto de 19 dos 21 Ministérios Públicos membros da AIAMP. Trata-se de uma rede de magistrados especializados em cibercrime, que tem o objetivo de promover e melhorar a informação disponível sobre os diferentes sistemas jurídicos ibero-americanos no âmbito da cibercriminalidade, potenciar o intercâmbio de experiências e conhecimentos necessários para solucionar os múltiplos problemas que se colocam nesta área, criar e difundir boas práticas entre os seus integrantes e otimizar e agilizar a cooperação institucional e as solicitações de cooperação judiciária internacional entre os vários países.

Foi ainda deliberado, pela XXIV Assembleia Geral da AIAMP, que esta rede seria um fórum de contacto e intercâmbio sobre tendências da cibercriminalidade e na obtenção de prova digital, devendo, para este efeito, realizar uma reunião anual dos respetivos pontos de contacto.

3. Este foi o contexto da realização da segunda reunião da CiberRede/*CiberRed* e foi também neste contexto que se escolheram os temas para discussão da conferência internacional, que procurou explorar a temática estratégica do cibercrime no espaço Ibero-Americano (fenómenos criminais e legislação), bem como a reação que os Ministérios Públicos e *Fiscalías* estão a adotar para fazer face a este desafio.

[1] Argentina, Brasil, Chile, Colômbia, Costa Rica, Cuba, Espanha, Guatemala, México, Panamá, Paraguai, Peru, Portugal e República Dominicana..

[2] Quanto ao representante do Uruguai, foi impedido de participar por razões de saúde, graves, de última hora.

4. Deixam-se de seguida as conclusões que a Coordenação da rede, assegurada por Portugal, retirou da realização da reunião.

B – AS NORMAS RESPEITANTES AO CIBERCRIME NO ESPAÇO IBERO-AMERICANO

5. Uma das conclusões mais visíveis da reunião respeitou à existência de quadros normativos, em matéria de cibercriminalidade, nos países do espaço ibero-americano. A este propósito, resultou da reunião que alguns dos países têm já quadros normativos específicos a este respeito (seja apelidando-os de crimes informáticos, crimes cibernéticos, ciberdelitos ou cibercrimes).
Porém, ainda assim não acontece com um número significativo de países, que apenas têm previsões de crimes mais genéricos, embora suscetíveis de serem cometidos nas redes. Nem sempre estes últimos se adaptam às novas realidades, sendo, portanto, necessária alguma inovação legislativa ou, pelo menos, algum ajustamento legal. Na maior parte destes casos, existe mesmo necessidade de introdução legislativa de crimes informáticos, ou cibercrimes, propriamente ditos. Alguns destes últimos países estão já a dar passos neste sentido inspirando-se, quer na Convenção de Budapeste, quer nas legislações de outros países do grupo.

C – AS NORMAS RESPEITANTES À OBTENÇÃO DE PROVA DIGITAL NO ESPAÇO IBERO-AMERICANO

6. A conclusão é mais pessimista no que respeita a normas respeitantes à obtenção de prova digital: apenas um pequeno número dos países ibero-americanos tem normas processuais especificamente dirigidas à obtenção de prova digital. Nalguns casos, os quadros normativos gerais têm sido aplicados ao ambiente digital, embora com insuficiência.
A este respeito, além da carência normativa, foi identificada também a necessidade de uma discussão mais aprofundada, de identificação das lacunas de cada um dos países.

7. Junta-se, como Anexo C, uma súmula dos quadros normativos dos diversos países presentes na reunião.

D – NECESSIDADES DE FORMAÇÃO ESPECÍFICA E DE ESPECIALIZAÇÃO NA INVESTIGAÇÃO

8. Noutra vertente, foi possível concluir que, de modo uniforme nos diversos países, os crimes nas redes de comunicações estão em grande expansão. Pela respetiva complexidade, requerem conhecimentos

especializados e meios específicos de investigação. Ficou clara a necessidade generalizada de formação de magistrados. Também foi recorrentemente afirmada a necessidade de atualização frequente daquela formação, porventura por via da partilha de conhecimentos e boas práticas entre magistrados, ou porventura por via de debate de casos práticos.

9. Por outro lado, foi vincada a necessidade de especialização de magistrados nesta área como uma das mais claras conclusões da reunião. Todavia, a forma como os diversos países enfrentam esta necessidade é dissonante, sendo o panorama muito diferenciado e existindo diversos modelos. Nalguns dos países ibero-americanos, esta especialização, que já existe, foi insistentemente afirmada com uma necessidade inevitável, por não ser possível investigar cibercriminalidade de outra forma.

10. A comparação entre os diversos modelos, com o cotejo das vantagens de uns e outros, permitiu que esta troca de experiências facultasse aos participantes pistas para evolução interna no futuro próximo. De entre os países representados, foi possível concluir que são seguidos por eles os seguintes diferentes modelos:

1. unidades nacionais especializadas de investigação centralizada;
2. unidades de coordenação nacional, com descentralização da investigação em pontos focais;
3. unidades de coordenação nacional (com incidência específica na formação e apoio remoto) e dispersão da investigação;
4. unidades nacionais de investigação (não especificamente especializadas);
5. unidades nacionais de apoio técnico, com dispersão da investigação e
6. inexistência de especialização.

D. 1) UNIDADES NACIONAIS ESPECIALIZADAS DE INVESTIGAÇÃO CENTRALIZADA

11. Nalguns dos Ministérios Públicos ou *Fiscalías* optou-se por concentrar as investigações numa estrutura de âmbito e competência nacional. Nela, de forma centralizada, são desenvolvidas as investigações, por um corpo especializado de procuradores ou *fiscales*. Assim sucede, por exemplo, na República Dominicana, desde 2013, altura em que foi instituída uma Unidade Especializada em Ciberdelito. Modelo parecido foi adotado pelo Paraguai, que igualmente criou uma unidade especializada, em Assunção, capital do país – embora, neste caso, esta unidade tenha também funções de apoio técnico.

D. 2) UNIDADES DE COORDENAÇÃO NACIONAL, COM DESCENTRALIZAÇÃO DA INVESTIGAÇÃO EM PONTOS FOCAIS

12. Noutros casos, apesar de os Ministérios Públicos ou *Fiscalías* terem criado uma unidade centralizada de coordenação, optaram por alocar as concretas investigações, de forma descentralizada, a *fiscales* ou procuradores distribuídos pelo território, embora com especialização. Desta forma, a unidade central assume assim preponderantemente funções de garantia da unidade de ação em todo o país e de atuação coordenada.

Este foi o modelo adotado em Espanha e em Portugal. Ambos os países têm uma unidade nacional, que coordena, mas as concretas investigações estão distribuídas a pontos de contacto especializados, dispersos pelo território. Alguns destes pontos de contacto trabalham exclusivamente em investigações nesta área, enquanto outros, sem embargo da especialização, assumem também outras funções (segundo as exigências da circunscrição territorial a que estejam adstritos).

Quanto à concreta coordenação, o modelo português é mais vocacionado para os métodos, enquanto o modelo espanhol incide também, além disso, na coordenação operacional e hierárquica dos pontos de contacto.

D. 3) UNIDADES DE COORDENAÇÃO (COM INCIDÊNCIA ESPECÍFICA NA FORMAÇÃO E APOIO REMOTO) E DISPERSÃO DA INVESTIGAÇÃO

13. Noutros casos, o modelo de coordenação nacional é mais vocacionado para o apoio remoto e para a formação dos procuradores ou *fiscales*. Isto é, havendo uma unidade nacional instituída, a vocação da mesma é sobretudo implementar a capacitação dos investigadores – que, de forma especializada ou não, consoante a opção local, assumem de forma dispersa as investigações.

Percebe-se que este tenha sido o modelo adotado por países com estrutura federal, como o Brasil e a Argentina, que cumulam a existência de um Ministério Público Federal com Ministérios Públicos dos Estados ou das Províncias. Em ambos os casos, há focos de especialização nalgumas circunscrições, não os havendo noutras, nas quais a investigação é feita, de forma dispersa, pelos vários procuradores.

Já no caso do Chile, a situação é mitigada: existe uma estrutura nacional de coordenação e apoio vocacionada para temáticas de cibercrime, que incorpora componentes técnicas, a quem compete apoiar *fiscales* de todo o país em investigações concretas. Porém, a par disso, há especialização ao nível local em temas de cibercriminalidade – há *fiscales* específicos a quem são atribuídas as investigações nesta área (cibercriminalidade e outra criminalidade relacionada com cartões bancários), embora tenham também outras competências funcionais.

D. 4) UNIDADES NACIONAIS DE INVESTIGAÇÃO (NÃO ESPECIFICAMENTE ESPECIALIZADAS)

14. Noutros casos, as temáticas de cibercriminalidade são assumidas por unidades nacionais especializadas – não especializadas em cibercrime, mas em assuntos mais genéricos e englobantes, como crime organizado, crime grave ou outros ainda mais específicos.

Em geral, estas unidades nacionais foram constituídas para fazer face a problemas específicos, relevantes no contexto local e, depois, com a emergência da temática da cibercriminalidade, veio a ser-lhes também acometida competência para investigar processos de investigação criminal desta natureza.

É o caso da Costa Rica, que tem uma *Fiscalía* Nacional especializada em fraudes, e que também investiga casos de cibercrime. Esta unidade nacional, tendo uma gama mais ampla de competências, tem também vocação para apoio e formação na área do cibercrime.

Mas é também o caso da Colômbia, que agregou a investigação de alguns casos de cibercrime a uma unidade nacional especializada na investigação de crime organizado. Porém, a competência desta unidade nacional não é exclusiva, havendo investigações de casos de cibercriminalidade dispersos pelas várias unidades territoriais do país.

No Panamá, a situação é similar: existe uma unidade especializada em crimes contra o direito de autor a quem tem sido conferida competência para a investigação de alguns casos de cibercriminalidade,

embora a investigação deste tipo de casos esteja igualmente dispersa, por outros departamentos do Ministério Público.

D. 5) UNIDADES NACIONAIS DE APOIO EXCLUSIVAMENTE TÉCNICO, COM DISPERSÃO DA INVESTIGAÇÃO

15. Alguns países optaram por criar unidades nacionais com mais vocação de apoio técnico (tecnológico), descentralizando a investigação criminal propriamente dita.

Assim aconteceu com o México, que criou uma unidade nacional de apoio meramente técnico, deixando que a investigação criminal se faça de forma dispersa, nos vários departamentos do território. A função desta unidade nacional é de mero apoio técnico aos investigadores, não lhe cabendo funções específicas de investigação e ação penal, nem de coordenação destas investigações.

A situação na Guatemala é próxima desta, embora a estrutura nacional especializada criada, embora incluindo esta valência, não seja exclusivamente vocacionada para o cibercrime.

D. 6) INEXISTÊNCIA DE ESPECIALIZAÇÃO

16. Finalmente, alguns dos países, ainda não estabeleceram qualquer forma de especialização do Ministério Público a este respeito, estados os casos concretos dispersos por todas as circunscrições territoriais. Assim acontece, designadamente, com o Peru e com Cuba.

E – A CiberRede/*CiberRed*

17. Noutra vertente, no que respeita à própria CiberRede/*CiberRed* e ao seu funcionamento e virtualidades, foram também formuladas conclusões.

E. 1) A IMPORTÂNCIA DA REDE

18. Reforçou-se, entre os participantes, a convicção da mais-valia da rede e das respetivas reuniões, por constituir um fórum permanente e especializado que facilita a troca de experiências e boas práticas entre colegas do Ministério Público . A este propósito, os participantes expressaram haver grande utilidade na realização de reuniões presenciais, mas também haveria vantagem em permitir o contacto permanente, por via de uma plataforma segura de comunicações eletrónicas.

Uma tal plataforma permitiria, de forma permanente, trocar informação não sensível entre os pontos de contacto – foi referenciada a possibilidade de utilizar a já existente plataforma *Iber@*, gerida pela *IberRed*, sendo referido que esta última está numa fase de menor estabilidade, em reformulação.

Uma plataforma de comunicações potenciaria, por exemplo, de forma tópica e específica, obter esclarecimentos de outros colegas pontos de contacto em casos concretos. Ou obter elementos de trabalho. Ou partilhar iniciativas de formação.

Não estando disponível uma plataforma segura para troca de informação, criou-se, como forma de provisoriamente assegurar contacto expedito, um grupo de Whatsapp, incluindo todos os pontos de contacto que se mostraram disponíveis para o efeito.

E. 2) A PARTILHA DE EXPERIÊNCIA E BOAS PRÁTICAS

19. Durante a reunião foram partilhados casos concretos de iniciativas, de alguns dos países representados, dos quais se descrevem alguns, em demonstração da potencialidade desta troca de experiência e boas práticas.

A República Dominicana, que se tem deparado com inúmeros casos de burlas do tipo *Business Email Compromisse* (que na Europa é mais conhecido como *CEO Fraud*), decidiu criar um manual de combate a este crime, que prevê a criação de um portal *web*, do Ministério Público, que centraliza informação em tempo real sobre este tipo de casos – este método tem permitido identificar as "*money mules*". Também por esta via, é prestada informação às vítimas sobre a melhor forma de reagir, quando este tipo de crime ocorre. Esta experiência pode ser potenciada se partilhada com outros Ministérios Públicos.
Ainda a República Dominicana, partilhou um "*Protocolo de investigación y procesamiento de casos de explotación sexual en línea de niños, niñas y adolescentes*", manual que pretende auxiliar todos os magistrados do Ministério Público na investigação de crimes de exploração sexual de crianças e jovens.
Por seu lado, o Brasil, partilhou que organizou um "Roteiro de investigação de crimes cibernéticos", o qual traduziu para espanhol, podendo assim ser utilizado em toda a Ibero América.
Por último, ainda a título de exemplo, o México elaborou e partilhou um "*Guia Técnica de Cadena de Custodia de Evidencia Digital*", manual técnico de apoio a investigações que suponham a recolha de prova digital.

20. Resultou claramente das discussões que haveria vantagem em vir a dinamizar um espaço dedicado a esta rede, na página *web* da AIAMP. Tal espaço deveria ser usado para divulgar a existência e potencialidades da *CiberRede/CiberRed*, mas também de outra informação pública ou publicável, como os manuais de boas práticas ou jurisprudência sobre cibercrime e prova digital.

E. 3) A TROCA DE INFORMAÇÃO OPERACIONAL

21. Noticia-se que vai ser brevemente apresentado à próxima reunião da COMJIB (Conferência de Ministros da Justiça da Ibero América), um projeto de tratado internacional destinado a regular a transmissão eletrónica de pedidos de auxílio judiciário mútuo entre os Estados da COMJIB.
Todavia, no presente momento, no espaço da AIAMP, não existe ainda quadro legal que permita a troca de pedidos de cooperação internacional em matéria penal, por via eletrónica. Portanto, vigora o método de uso das clássicas cartas rogatórias, transmitidas em papel, entre as Autoridades Centrais de cooperação internacional.

22. Não obstante, a CiberRede/*CiberRed* pode vir a ser usada, desde já e no corrente contexto, para apoio técnico, entre os diversos pontos de contacto, bem como para trocas informais, à margem de pedidos formais de cooperação.

A este propósito, de transmissão de informação operacional, foi sublinhada a utilidade que pode vir a ter o Acordo de Cooperação Interinstitucional celebrado na Assembleia Geral da AIAMP do México, em 2018.
Aliás, foi igualmente sublinhado que a CiberRede/*CiberRed* é o fórum adequado para, no seio da AIAMP, vir a ser futuramente discutida a possibilidade de criação de ferramentas de cooperação internacional, específicas para a obtenção de prova digital.

E. 4) A CONSOLIDAÇÃO DOS PONTOS DE CONTACTO

23. Como se disse, a CiberRede/*CiberRed* conta com pontos de contacto representando 19 dos 21 países da AIAMP. Ou seja, há ainda dois Ministérios Públicos da AIAMP[3] que não indicaram representantes seus como pontos de contacto.
A primeira reunião da rede, em Lisboa, contou com representantes de 18 países membros. A segunda reunião apenas contou com representantes de 15 países membros.
Verificou-se que, entre a primeira e a segunda reunião, alguns dos pontos de contacto transitaram para posições funcionais diferentes das que tinham antes, deixando de assegurar a função de pontos de contacto. Muito deles não deram conta dessa circunstância à Coordenação da REde, tendo por isso sido necessário solicitar a sua substituição em data próxima da reunião. Ainda, quando a alguns dos pontos de contacto, não foi mesmo possível estabelecer com eficácia comunicação, a propósito da realização da reunião.
Importaria, pois, sensibilizar os Procuradores-Gerais e Fiscais-Gerais, aquando da próxima assembleia geral da AIAMP, para o crescente papel e relevância desta rede, e para a importância de consolidar as funções de pontos de contacto.

E. 5) QUADROS NORMATIVOS NA ÁREA DO CIBERCRIME E DA PROVA DIGITAL

24. A CiberRede/*CiberRed* tem assumido, desde o primeiro momento, que um dos vetores mais importantes para facilitar a cooperação internacional é a harmonização das diversas legislações. Por isso, tem sido incluída nas discussões a troca de impressões quanto aos quadros normativos dos diversos países, em temas de cibercrime e prova digital. Somente conhecendo o quadro normativo daqueles países com quem se coopera será possível maximizar as ferramentas de cooperação internacional.
Manifestaram os participantes na reunião ser pois importante, com vista a intensificar o conhecimento das leis de outros países, desenvolver um breve trabalho de estudo comparativo de leis, na área do cibercrime e da prova digital. Tal estudo poderá ser efetuado partindo de questionários, a distribuir pelos pontos de contacto.

E. 6) A SUSTENTABILIDADE DA REDE

25. As duas reuniões dos pontos de contacto da CiberRede/*CiberRed* (realizadas em Lisboa, em fevereiro de 2018 e em Santiago, Chile, em junho de 2019), tiveram o apoio do Programa GLACY+ do Conselho da Europa. O apoio deste programa, que conta com fundos da União Europeia, permitiu custear as deslocações dos pontos de contacto, bem como o respetivo alojamento e alimentação. Também foi este programa que, no caso de Santiago, custeou as despesas como o local de realização da reunião (o qual, no caso da reunião de Lisboa, foi facultado pela Procuradoria-Geral da República de Portugal).

[3] A Nicarágua e a Venezuela.

Desta forma, foi possível realizar as duas reuniões sem que as mesmas supusessem qualquer encargo financeiro para os participantes ou para as Procuradorias-Gerais e *Fiscalias*.
Importava, porém, ponderar soluções de sustentabilidade da rede, procurando-se outras fontes de financiamento, que assegurem continuidade e autonomia.

8 de outubro de 2019

ANEXO A

Conferencia Internacional y 2ª Reunión Anual de CiberRed

RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA

Conferência Internacional e 2ª Reunião Anual da CiberRede

REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME

Santiago de Chile, 25 e 26 de Júnio de 2019
Santiago do Chile, 25 e 26 de junho de 2019

LISTA DE PARTICIPANTES

País	Nome	Cargo
ARGENTINA	**Horacio Azzolín**	*Unidad Especializada en Ciberdelincuencia*
BRASIL	**Fernanda Domingos**	Grupo de Trabalho sobre Crimes Cibernéticos
BRASIL	**Neide de Oliveira**	Coordenadora do Grupo de Trabalho sobre Crimes Cibernéticos
CHILE	**Antonio Segovia Arancibia**	*Fiscalía Nacional - Director – Unidad de Cooperación Internacional y Extradiciones*
CHILE	**Camila Bosch**	*Fiscalía Nacional - Unidad de Cooperación Internacional y Extradiciones*
CHILE	**Constanza Encina**	*Fiscalía Regional Oriente Alta Complejidad*
CHILE	**Eduardo Baeza**	*Fiscal adjunto*
CHILE	**Giovanna Herrera**	*Fiscal adjunto*
CHILE	**Luis Herrera**	*Fiscalía Regional Sur Puente Alto*
CHILE	**Mauricio Fernández Montalbán**	*Director-Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado (Fiscalía Nacional)*
CHILE	**Monserrat Ramirez**	*Fiscalía Nacional - Unidad de Cooperación Internacional y Extradiciones*
COLOMBIA	**Luis Orlando Paloma Parra**	*Fiscal del eje de cibercriminalidad de la Dirección contra las organizaciones criminales*
COSTA RICA	**Carlos Castro Sojo**	*Fiscal – Unidad Ciberdelito – Oficina de Fraudes*
CUBA	**Dimas Herrera Gandol**	*Secretaria del Fiscal General*
ESPAÑA	**Ana Maria Martín**	*Fiscal de Criminalidad Informática*
ESPAÑA	**Elvira Tejada**	*Fiscal de Sala de Criminalidad Informática*

GUATEMALA	**Andrea Lisbeth Mejia Mendez**	*Departamento de Ciber Delito*
GUATEMALA	**María Elena Galvez Rafael**	*Jefa del Departamento de Ciber Delito*
MÉXICO	**Marco Mecalco Raya**	*Unidad de Investigaciones Cibernéticas*
PANAMÁ	**Martín Oscar Rodriguez Lezcano**	*Fiscal Especializado en Delitos Contra la Propiedad Intelectual y Seguridad Informática*
PARAGUAY	**María Soledad Machuca Vidal**	*Fiscal Adjunta encargada de la Unidad Especializada de Delitos Informáticos del Ministerio Público*
PERÚ	**Ángela Olivia Arévalo Vásquez**	*Fiscal - Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación*
PORTUGAL	**Pedro Verdelho**	Coordenador do Gabinete Cibercrime
REPÚBLICA DOMINICANA	**Iván Féliz Vargas**	*Procurador General de Corte, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología*
COUNCIL OF EUROPE	**Manuel de Almeida Pereira**	*Project Manager* *Cybercrime Programme Office (C-PROC)*
COUNCIL OF EUROPE	**Andrei-Stefan Candrea**	*Project Assistant* *Cybercrime Programme Office (C-PROC)*

ANEXO B

Conferencia Internacional y 2ª Reunión Anual de CiberRed

RED IBEROAMERICANA DE FISCALES ESPECIALIZADOS EN CIBERDELINCUENCIA

Conferência Internacional e 2ª Reunião Anual da CiberRede

REDE IBERO-AMERICANA DE MINISTÉRIOS PÚBLICOS ESPECIALIZADOS EM CIBERCRIME

Santiago de Chile, 25 e 26 de Júnio de 2019
Santiago do Chile, 25 e 26 de junho de 2019

CONFERENCIA INTERNACIONAL 25 DE JUNIO	CONFERÊNCIA INTERNACIONAL 25 DE JUNHO
10:00 – Inauguración *Representante del Ministerio Público de Chile* *Representante del Consejo de Europa* *Representante de Unión Europea*	**10:00 – Abertura** *Representante do Ministério Público do Chile* *Representante do Conselho de Europa* *Representante da União Europeia*
SESIÓN 1 – EL CIBERDELITO EN EL ESPACIO IBEROAMERICANO **10:15 – El marco internacional de la ciberdelincuencia: la Convención de Budapest – *Pedro Verdelho - Portugal* (***Breve presentación e intervención de los participantes)*** **11:00** – Pausa **11:15 - El panorama legislativo en el ámbito del ciberdelito y de la obtención de prueba digital, en los países miembros de AIAMP** *Sesión con intervención de los participantes* **13:00** – Pausa	**SESSÃO 1 – O CIBERCRIME NO ESPAÇO IBEROAMERICANO** **10:15 – Enquadramento internacional do cibercrime: a Convenção de Budapeste – *Pedro Verdelho - Portugal* (***Breve apresentação e intervenção dos participantes)*** **11:00** – Pausa **11:15 – O panorama legislativo na área do cibercrime e da obtenção de prova digital, nos países membros da AIAMP** *Sessão com intervenção dos participantes* **13:00** – Pausa
SESIÓN 2 – COOPERACIÓN EN LA OBTENCIÓN DE PRUEBA DIGITAL **14:30 – La Convención de Budapest: instrumentos específicos y la rede 24/7 – *Elvira Tejada - España*** *(Breve presentación e intervención de los participantes)* **15:30** – Pausa **15:45 – Experiencias y buenas prácticas:** **a) cooperación con operadores de comunicaciones nacionales y**	**SESSÃO 2 – COOPERAÇÃO NA OBTENÇÃO DE PROVA DIGITAL** **14:30 – A Convenção de Budapeste: instrumentos específicos e a rede 24/7 – *Elvira Tejada - Espanha*** *(Breve apresentação e intervenção dos participantes)* **15:15** – Pausa **15:30 – Experiências e boas práticas:** **a) cooperação com operadores de telecomunicações nacionais e**

globales - *Neide de Oliveira e Fernanda Domingos - Brasil* b) equipos conjuntos de investigación *-Ana María Martin - España* *Breves presentaciones e intervención de los participantes* **17:30** - cierre del día	globais - *Neide de Oliveira e Fernanda Domingos - Brasil* b) equipas conjuntas de investigação - *Ana Maria Martin - Espanha* *Breves apresentações e intervenção dos participantes* **17:30** – encerramento do dia
CONFERENCIA INTERNACIONAL 26 DE JUNIO	**CONFERÊNCIA INTERNACIONAL 26 DE JUNHO**
SESIÓN 3 - EL MINISTERIO PÚBLICO Y LAS EXIGENCIAS DEL CIBERDELITO **10:00 - Estructuras especializadas del Ministerio Público, en el área del Ciberdelito** *Sesión con intervención de los participantes* **11:30 –** Pausa **11:45 – Cooperación Internacional de los Ministerios Públicos y Fiscalías de Iberoamérica - *António Segovia - Chile*** **12:30 – El Ministerio Público e el desafío del ciberdelito - *Pedro Verdelho - Portugal*** **13:00** – Cierre	**SESSÃO 3 – O MINISTÉRIO PÚBLICO E AS EXIGÊNCIAS DO CIBERCRIME** **10:00 – Estruturas especializadas do Ministério Público, na área do Cibercrime** *Sessão com intervenção dos participantes* **11:30** – Pausa **11:45 – Cooperação Internacional dos Ministérios Públicos e *Fiscalías* da Ibero-América – *António Segovia – Chile*** **12:30 - O Ministério Público e o desafio do cibercrime - *Pedro Verdelho - Portugal*** **13:00** – Encerramento
2ª REUNIÓN ANUAL DE CIBERRED 26 DE JUNIO	**2ª REUNIÃO ANUAL DA CIBERREDE 26 DE JUNHO**
14:30 – Inauguración **TEMA GENERAL: *CiberRed* EN EL PRÓXIMO TRIENIO: DESAFÍOS** **14:35 – Objetivos estratégicos de *CiberRed* para el próximo trienio** *Intervención de los participantes* **15:00 - Necesidades de formación especializada** *Intervención de los participantes* **15:30 – La próxima reunión de CiberRed: tema y formato** *Intervención de los participantes* **16:00** – Conclusiones y cierre	**14:30 – Abertura** **TEMA GERAL:– A *CiberRede* NO PRÓXIMO TRIÉNIO: DESAFIOS** **14:35 – Objetivos estratégicos da *CiberRede* para o próximo triénio** *Intervenção dos participantes* **15:00 – Necessidades de formação especializada** *Intervenção dos participantes* **15:30 – A próxima reunião da *CiberRede*: tema e formato** *Intervenção dos participantes* **16:00 – Conclusões e encerramento**

ANEXO C

CIBERCRIME E PROVA DIGITAL

SÚMULA DOS QUADROS NORMATIVOS

	NORMAS EM VIGOR	PROJETOS LEGISLATIVOS
ARGENTINA	O *Código Penal*, por via da *Ley 26388* (http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm) e da *Ley 26904* (http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm) inclui a maior parte dos tipos de crime da Convenção de Budapeste. Foi recentemente introduzida legislação interna que incrimina a mera posse de pornografia infantil. Não existem normas específicas sobre prova digital, uma vez que o *Código Procesal Penal*, alterado pela *Ley* 27063 (http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239340/norma.htm#28), apenas inclui, nos artigos 143 e 144, a interceção de comunicações e a apreensão de dados.	Existe um projeto de alteração do *Código Penal*, para passar a incluir novas condutas (como por exemplo a *revenge porn* e o uso de identidade falsa na Internet – existem muitos casos de uma e outra situação). Existem planos para ajustar o *Código Procesal Penal*.
BOLIVIA	Não existem tipos específicos de crimes neste campo – apenas, no Código Penal, um crime de manipulação informática de dados e de alteração, acesso e uso indevido de dados. Não existem normas específicas sobre prova digital – aplicam-se, dentro do possível, as normas gerais.	*OBS: informação recolhida na primeira reunião da CiberRede*
BRASIL	A Lei 12737 (https://www.jusbrasil.com.br/topicos/10605134/artigo-266-do-decreto-lei-n-2848-de-24-de-fevereiro-de-1891) introduziu no Código Penal (Artigos 154-A, 154-B, 266 e 313-A) os crimes de acesso ilegítimo, difusão ilícita de dispositivos e ataques de denegação de	Está pendente no Senado o Projeto de Lei PL 236/2012 (projeto de novo Código Penal), que prevê os crimes da Convenção de Budapeste (https://www25.senado.leg.br/web/atividade/materias/-/materia/106404/pdf).

	serviço. Ainda criminalizou a falsificação de cartões de crédito. Recentemente foi introduzido no Código Penal o Artigo 218º-C (pornografia de vingança), que já está em vigor. O Estatuto da Criança e Adolescente (https://presrepublica.jusbrasil.com.br/legislacao/91764/estatuto-da-crianca-e-do-adolescente-lei-8069-90#art-240), nos artigos 240, 241-A, 241-B, 241-C e 241-E, prevê a punição de pornografia infantil. Não existem normas específicas sobre prova digital. Foi publicada, entretanto, a Lei de Proteção de Dados, a qual entrará em vigor no ano de 2020.	
CHILE	A Lei Nº 19.223, de 1993 (http://bcn.cl/1uw5c), tipifica figuras penais relativas à informática. O Código de Processo Penal tem algumas normas aplicáveis à obtenção de prova digital (nos Artigos 222 a 226bis), designadamente sobre interceção de comunicações.	Está presentemente em discussão no Senado um projeto de lei de alteração do quadro penal substantivo, que tem em vista adotar todas as normas previstas na Convenção de Budapeste (*Boletín Nº* 10145-07 - http://www.senado.cl/appsenado/templates/tramitacion/index.php). Está igualmente em discussão um projeto de lei de revisão da Lei 20.009 (o seu processo está mais avançado e mais próximo do seu final) que, além de norma processuais respeitantes a prova digital, incorpora também normas substantivas referentes a ilícitos relacionados com cartões de crédito.
COLOMBIA	O Código Penal (alterado pela Lei 1273, de 5 de janeiro de 2009, também chamada Lei de Delitos Informáticos,) inclui nove delitos informáticos puros e outros mistos. Não existem na lei normas específicas sobre prova digital.	Está em discussão um projeto de lei de alteração do Código Penal, que introduzirá a burla informática – como um crime cometido no meio informático (*Projecto Lei 60/2018* da Câmara e *Projecto Lei 74/2018* do Senado). Este projeto vai incluir uma circunstância agravante no tipo de crime da burla, como forma de passar a incriminar-se a burla informática. Também inclui normas que punem o *sexting* e a *sextortion* (por via de uma circunstância agravante do crime de extorsão) e outras que punem o mero

		uso de *malware* – que presentemente não é punido. Foi aprovada a Lei 19/28, de adesão à Convenção de Budapeste e a Corte Constitucional já deu voto de exequibilidade desta lei, permitindo assim que o país venha a depositar o seu instrumento de ratificação da Convenção – o que será feito em breve.
COSTA RICA	O Código Penal contém uma secção específica que inclui delitos informáticos e conexos. Não há normas processuais específicas a este propósito, mas o princípio de liberdade probatória permite a obtenção de prova digital – com limites no acesso a certo tipo de prova, como por exemplo a interceção de comunicações.	Está pendente na Assembleia Legislativa um projeto de lei que visa rever os tipos de crime existentes, ao encontro das previsões da Convenção de Budapeste.
CUBA	Não existem tipos específicos de crimes neste domínio (o Código Penal data de 1980). Não existem normas específicas sobre prova digital (o Código de Processo Penal data de 1977).	Estão em fase de estudo, ainda não público, novos códigos Penal e de Processo Penal que irão incluir aspetos relacionados com as tecnologias. Após a revisão constitucional de abril de 2019, foi estipulado o prazo de 18 meses para a revisão daqueles dois diplomas. Por outro lado, está igualmente em estudo um diploma normativo que visa regular a informatização da sociedade, que vai igualmente impulsionar aquelas revisões.
EL SALVADOR	A Lei Especial Contra Delitos Informáticos e Conexos (Decreto 260, de 2016) inclui muitos tipos de ilícito – e também todos os previstos na Convenção de Budapeste. Existem diversas normas respeitantes a obtenção de prova digital, no Código Processual Penal (Decreto 733 de 2009), e em leis especiais: Decreto 953, de 2015 (lei especial contra a extorsão), Decreto 108, de 2006 (terrorismo) e Lei Especial para as Interceções Telefónicas.	*OBS: informação recolhida na primeira reunião da CiberRede*
ESPANHA	O *Código Penal Español* transpõe as normas penais substantivas previstas na Convenção de Budapeste.	Está pendente no parlamento uma proposta legislativa de incriminação da *suplantación de identidad*.

	A *Ley de Enjuiciamiento Criminal*, após a alteração da LO 13/2015, de 5 de outubro por sua vez, transpõe as normas processuais da Convenção.	Está também em análise uma nova lei integral da proteção da infância e da adolescência, que inclui normas respeitantes à proteção de menores nas redes (por exemplo, respeitantes ao incitamento ao suicídio ou à auto mutilação, através da rede). Existe um outro projeto legislativo em estudo, destinado a regular a retirada de conteúdos ilícitos nas redes (bloqueio de conteúdos, interrupção de serviços ou retirada de conteúdos *online*).
GUATEMALA	Não existem ainda tipos específicos de crimes neste campo. Também não existem normas específicas sobre prova digital.	Está pendente, no Congresso, um projeto legislativo com o específico propósito de transpor a Convenção de Budapeste. Aguarda a passagem do corrente período eleitoral.
HONDURAS	Não existem específicos crimes neste campo, no Código Penal - apenas crimes respeitantes à segurança das redes. Não existem normas específicas sobre prova digital.	*OBS: informação recolhida na primeira reunião da CiberRede*
MÉXICO	Existe um Código Penal Federal e diversos Códigos Penais dos Estados (um para cada Estado), que incluem normas na área do cibercrime. Apesar de haver um único código processual penal, a nível nacional, não existem normas específicas sobre prova digital.	
PANAMÁ	Ainda não existem um corpo consolidado de tipos específicos. Não existem normas específicas sobre prova digital.	Existe um projeto legislativo que visa adequar a legislação nacional à Convenção de Budapeste. Foi introduzido no Congresso em 2017.
PARAGUAY	Lei 4439, de 2011, consagra já algumas normas penais de acordo com a Convenção de Budapeste.	

	Não existem normas específicas sobre prova digital.	
PERÚ	A lei interna (Lei 80086) cobre todas as normas substantivas da Convenção de Budapeste e, bem assim, todas as suas normas processuais.	A Resolução Legislativa 30913, de fevereiro de 2019, aprovou a adesão à Convenção de Budapeste, sendo seguida, em Março de 2019, pela ratificação do executivo.
PORTUGAL	A Lei do Cibercrime (Lei 109/2009) transpõe todas as normas da Convenção de Budapeste – substantivas, processuais e de cooperação internacional.	
REPÚBLICA DOMINICANA	A lei interna (Lei 5307), transpõe todas as normas substantivas e processuais da Convenção de Budapeste.	Está em análise no Congresso, em sede de comissão especializada, um projeto de modernização da lei vigente.
URUGUAY	Não existem tipos específicos de crimes neste campo. Não existem na lei normas específicas sobre prova digital - apenas se prevê, em termos gerais, no Código de Processo Penal, a interceção de comunicações.	Existe um projeto legislativo que introduzirá alguns dos crimes descritos na Convenção de Budapeste (acesso não autorizado, dano informático e burla informática). Este projeto está ainda em fase de aprovação pelo poder executivo, somente sendo depois disso submetido ao Congresso. *OBS: informação recolhida na primeira reunião da CiberRede*