



SÉTIMA REUNIÃO
da
CiberRed
e
CONFERÊNCIA INTERNACIONAL

(23 a 25 de maio de 2023)

CONCLUSÕES DA COORDENAÇÃO

SÉTIMA REUNIÃO DA CiberRed e CONFERÊNCIA INTERNACIONAL CONCLUSÕES DA COORDENAÇÃO

A - A REUNIÃO

1. Decorreu, a 25 de maio de 2023, em Brasília (Brasil), a sétima reunião da *CiberRed*, a Rede Ibero-Americana de Ministérios Públicos Especializados em Cibercrime. Conjugadamente com ela, a 23 e 24 de maio, decorreu uma conferência internacional sobre o Segundo Protocolo Adicional à Convenção de Budapeste, dirigida aos pontos de contacto da rede¹. Estiveram presentes 27 participantes, que representaram 16 países da AIAMP², apenas não tendo estado representados Andorra, a Bolívia, Cuba, a Nicarágua³ e a Venezuela. Junta-se, como Anexo A, a lista de participantes na reunião da *CiberRed*, como Anexo B, a agenda da Conferência Internacional e, como Anexo C, a agenda da reunião da *CiberRed*.

2. A *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 em 20, dos 21 Ministérios Públicos membros da AIAMP.



Trata-se de uma rede de magistrados do Ministério Público 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

¹ Na Conferência participaram também os pontos de contacto do Fórum Cibercrime dos Ministérios Públicos dos Países da CPLP e ainda procuradores e juízes brasileiros.

² Argentina, Brasil, Chile, Colômbia, Costa Rica, El Salvador, Equador, Espanha, Guatemala, México, Panamá, Paraguai, Perú, Portugal, República Dominicana e Uruguai.

³ A Nicarágua nunca indicou pontos de contacto para a *CiberRed*.

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 permanente 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. A primeira reunião da *CiberRed* realizou-se a 5 de fevereiro de 2018, em Lisboa, Portugal, e a segunda a 25 e 26 de junho de 2019, em Santiago, Chile.

Durante o período da pandemia resultante da COVID-19, suspenderam-se as reuniões presenciais, mas realizaram-se reuniões por videoconferência a 18 de setembro de 2020, 17 de dezembro de 2020, 21 de maio de 2021 e 15 de julho de 2022.

4. Este foi o contexto da realização da sétima reunião da *CiberRed*, já completamente em formato presencial, e foi também neste contexto que se escolheram os temas para discussão da conferência internacional, que procurou explorar uma temática muito atual, relacionada com a possível adesão de muitos dos Estados da Ibero-América ao Segundo Protocolo Adicional à Convenção de Budapeste (alguns deles já assinaram o protocolo).

B – A CONFERÊNCIA INTERNACIONAL

5. A Conferência Internacional sobre o Segundo Protocolo Adicional à Convenção de Budapeste decorreu a 23 e 24 de maio de 2023. A sua realização foi conjugada com a reunião da *CiberRed* para permitir aos respetivos pontos de contacto alargar o seu conhecimento sobre aquele muito recente, mas

extremamente relevante, marco da cooperação internacional na área da cibercriminalidade.



6. A Convenção de Budapeste é o incontornável instrumento internacional na área da cibercriminalidade e da obtenção da prova digital. Prevê normas de direito penal substantivo e normas processuais que devem ser implementadas ao nível doméstico.

Inclui também normas de cooperação internacional específicas para este tipo de criminalidade e prova, as quais complementam normas já em vigor, por força de outros tratados internacionais.

Embora a Convenção de Budapeste se mantenha atual, a verdade é que o contexto e realidade em seu redor evoluíram: os fornecedores de serviço globais, a deslocalização da informação, o armazenamento na chamada “nuvem”, as técnicas de anonimização e a Darkweb, alteraram as formas de investigar crimes em que se requeira prova digital e trouxeram novas exigências às autoridades de justiça criminal. Este, foi o contexto em que surgiu o Segundo Protocolo Adicional à Convenção de Budapeste, negociado entre 2017 e 2021 e aberto à assinatura a 12 de maio de 2022, em Estrasburgo.

7. Um dos propósitos da conferência internacional foi o de permitir aos participantes alargar o seu conhecimento sobre o Segundo Protocolo e sobre as respetivas consequências práticas, na investigação criminal. Embora o Segundo Protocolo Adicional à Convenção de Budapeste ainda não esteja em vigor⁴, é já muito relevante, porque oito dos membros da *CiberRed* (Andorra, Argentina, Chile, Colômbia, Costa Rica, Espanha, Portugal e República Dominicana) assinaram já o protocolo⁵, esperando-se, portanto, que o venham a ratificar em breve.

8. Durante a Conferência foi feito o enquadramento da Convenção de Budapeste, bem como se identificaram consequências da adesão à mesma ao nível interno, dos Estados-Parte.

Por outro lado, foi apresentado o Segundo Protocolo Adicional. Quanto a este, foram explorados alguns dos mecanismos de obtenção de prova que nele se preveem. Foi o caso da cooperação direta com prestadores de serviços globais, e foi também o caso das possibilidades de obtenção de prova digital em situações de emergência. Foram ainda explicadas as particularidades de utilização da videoconferência e das equipas conjuntas de investigação, no contexto do Protocolo.

9. Outro dos aspetos relevantes abordados foi o da cooperação que as autoridades de justiça criminal podem obter da ICANN (*Internet Corporation for Assigned Names and Numbers*).

Os participantes na reunião sugeriram a replicação desta específica sessão, focando a cooperação da ICANN nas investigações criminais, numa outra sessão, futuramente organizada pela *CiberRed*, destinada em geral a procuradores da Ibero-América.

10. Foi ainda feita uma apresentação sobre as atividades da REDTRAM da AIAMP (*Red Iberoamericana de Fiscales Especializados en Trata de Personas y Tráfico Ilícito de Migrantes*), pela ligação que as atividades daquela rede podem ter ao ciberespaço. Os participantes na reunião sublinharam a vantagem que poderá haver na realização de iniciativas conjuntas da *CiberRed* com esta outra rede da AIAMP.

C – A REUNIÃO DE PONTOS DE CONTACTO DA CIBERRED

11. Deixam-se de seguida algumas das conclusões mais importantes anotadas durante a reunião, pela Coordenação da rede, assegurada por Portugal.

C.1. AS ESTRUTURAS ESPECIALIZADOS EM CIBERCRIME NO MINISTÉRIO PÚBLICO

12. Foi nota unânime, entre todos os participantes que, de modo uniforme nos diversos países, os crimes nas redes de comunicações estão em grande expansão. Por esse motivo e pela respetiva complexidade, é também unanimemente reconhecida a necessidade de se organizarem, no Ministério Público, estruturas especializadas e meios específicos de investigação. A par, ficou clara a necessidade generalizada de formação de magistrados nesta área. 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.

⁴ Nesta data apenas a Sérvia depositou o seu instrumento de ratificação, sendo requeridas pelo menos cinco ratificações para que o Protocolo entre em vigor.

⁵ Pode consultar-se a lista atualizada dos signatários do Protocolo aqui: <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224>.

13. Um dos temas expressamente incluído na agenda foi precisamente o da necessidade de especialização de magistrados nesta área. Esta sessão foi aliás uma das mais vivas da reunião. A este propósito sublinhou-se a necessidade de cada um dos países refletir sobre o modelo que mais se adequa à sua realidade. Perante o aumento exponencial deste tipo de criminalidade, a especialização tem que ser criteriosamente aplicada, para evitar que grandes massas de casos sejam atribuídas às unidades especializadas, tornando-as assim macrocéfalas ou inoperantes.

14. Como nota de claro progresso, em relação a reuniões anteriores, foi verificado que a generalidade dos países representados na reunião considera já, de alguma forma, a especialização, embora adotando modelos muito



variáveis. Por toda a região da Ibero-América convivem unidades nacionais especializadas (de investigação centralizada nuns casos, de descentralização da investigação em pontos focais, noutros), unidades de mera coordenação nacional (por exemplo, com mais incidência na formação e apoio remoto às investigações, dispersas pelo território), unidades nacionais de investigação (não especializadas especificamente em cibercrime, mas juntando este fenómeno a outros mais complexos), e meras unidades de apoio tecnológicos às investigações dispersas por todo o território.

C.2. A IMPLEMENTAÇÃO DO SEGUNDO PROTOCOLO ADICIONAL

15. Outro dos temas introduzidos na agenda foi o da implementação, no concreto, do Segundo Protocolo Adicional à Convenção de Budapeste.

Este tratado internacional supõe a criação de normas internas que permitam, por um lado, obter prova digital de outros países, por outro, permitir que autoridades de outros países obtenham prova digital alojada num servidor nacional.

Uma das questões que supõe mais reflexão é a de quem devam ser as autoridades nacionais a intervir no processo.

16. O artigo 7º do Protocolo prevê a possibilidade de remessa direta de pedidos de informação, de uma autoridade justiça criminal de um país, a um fornecedor de serviços noutro país. Também, a possibilidade de se exigir a notificação prévia a autoridades nacionais. Por sua vez, no artigo 8º do Protocolo é mesmo obrigatório que exista esta autoridade nacional designada, uma vez que a ela compete dar execução a pedidos internacionais. Esta execução pode supor análise jurídica e decisão judiciária, razão pela qual se infere que esta autoridade tenha que estar inserida no poder judiciário. De facto, é-lhe exigida uma intervenção que ocorrerá, por exemplo, aquando da implementação, a nível doméstico, de uma ordem direta, estrangeira, de obtenção de informações, emitida por uma entidade judiciária, destinada a um fornecedor de serviço noutro Estado (artigo 8º do Protocolo).

De facto, a intervenção das autoridades nacionais a este respeito supõe o exercício de poderes jurisdicionais. Por isso, é recomendável que as autoridades que venham a ser designadas para este efeito sejam autoridades judiciárias – em geral, no contexto da Ibero-América, tal autoridade deverá ser o

Ministério Público. Pela redação do Protocolo, parece excluída a possibilidade de que as funções em causa sejam desempenhadas por autoridades administrativas, pertencentes à administração pública ou ao executivo. Esta foi aliás a posição consensual da generalidade dos participantes na reunião.

A questão é pertinente porque, nalguns dos países do espaço Ibero-Americano, a cooperação internacional é ainda liderada por autoridades centrais baseadas no Ministério da Justiça – e não no Ministério Público. As tarefas da incumbência das “autoridades nacionais”, no contexto do Segundo Protocolo Adicional, nalguns casos, estão claramente fora da esfera de Ministérios da Justiça, antes se inserindo, claramente, na esfera jurisdicional do Ministério Público.

C.3. CRIPTOATIVOS

17. Constava também da agenda a apresentação de um roteiro de atuação, em investigação criminal, referente a criptoativos, recentemente publicado pelo Ministério Público Federal do Brasil.

Esta apresentação deu origem a uma interessante discussão a propósito das investigações criminais que, de alguma forma, se relacionam com esta realidade. Para além do manual brasileiro, foi referido um outro, emitido pelo Ministério Público Federal da Argentina. Além disso, foram apresentadas diversas experiências práticas.

O grupo concluiu que a dimensão e complexidade das questões suscitadas a este respeito justificariam um trabalho mais alargado sobre a matéria.

C.4. DADOS DE ASSINANTE E ENDEREÇOS DE IP

18. Embora não constasse da agenda, pela relevância que tem ao nível da cooperação internacional, e por estar relacionado com o artigo 7º do Segundo Protocolo Adicional à Convenção de Budapeste, discutiu-se muito a possibilidade de obtenção transfronteiriça de informação sobre endereços de IP. É informação muito relevante nas concretas investigações e o grupo concluiu que a importância deste tema justificava a realização de trabalho adicional a este respeito.



C.5. A CONSOLIDAÇÃO DA REDE DE PONTOS DE CONTACTO

19. Como se disse, a *CiberRed* conta com pontos de contacto representando 20 dos 21 países da AIAMP. Ou seja, há ainda um dos Ministérios Públicos da AIAMP⁶ que não indicou representantes seus como pontos de contacto. A presença dos diversos pontos de contacto tem sido variável, nas reuniões (em geral, têm participado entre 15 e 18 representantes dos países membros).

Verifica-se que, entre reuniões, alguns dos

pontos de contacto transitam para posições funcionais diferentes das que tinham antes, deixando de assegurar a função de pontos de contacto. Muito deles não dão conta dessa circunstância à Coordenação da Rede ou à Secretaria da AIAMP, tendo por isso sido necessário solicitar a sua substituição em data

⁶ A Nicarágua.



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.

C.6. A SUSTENTABILIDADE DA REDE

20. As três reuniões presenciais dos pontos de contacto da *CiberRed* (realizadas em Lisboa, em fevereiro de 2018, em Santiago, em junho de 2019 e em Brasília, em maio de 2023), 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 e no caso de Brasília foi facultado pela Procuradoria-Geral da República do Brasil). Desta forma, foi possível realizar as três reuniões sem que as mesmas supusessem qualquer encargo financeiro para os participantes ou para as Procuradorias-Gerais e *Fiscalias*. Trata-se de um financiamento ocasional, dependente de circunstâncias conjunturais. Importava, por isso, ponderar soluções de sustentabilidade da rede, procurando-se outras fontes de financiamento, que assegurem sustentabilidade, continuidade e autonomia.

5 de junho de 2023

ANEXO A

LISTA DE PARTICIPANTES

País	Nome	Cargo
ARGENTINA	Matias Grondona	Ministerio Público Fiscal de la Nación Subsecretario Administrativo
BRASIL	Anamara Osório Silva	Procuradora Federal Procuradoria-Geral da República
BRASIL	Fernanda Domingos	Procuradora Regional Grupo de Trabalho sobre Crimes Cibernéticos
BRASIL	Neide de Oliveira	Procuradora Regional Grupo de Trabalho sobre Crimes Cibernéticos
BRASIL	Thiago Augusto Bueno	Procurador Federal
CHILE	Antonio Segovia Arancibia	<i>Fiscalía Nacional - Unidad de Cooperación Internacional y Extradiciones</i>
CHILE	Mauricio Fernández Montalbán	<i>Fiscalía Nacional - Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado</i>
COLÔMBIA	Edna Patricia Cabrera Londoño	<i>Fiscalía General de la Nación Directoria Especializada contra los Delitos Informáticos</i>
COSTA RICA	Esteban Aguilar Vargas	Ministerio Público Coordinador Jefe de la Unidad de Cibercrimen
EL SALVADOR	Duglas Gilberto Espinal Claros	Fiscalia General DE la Republica de El Salvador Jefe de Unidad de Análisis de Información Fiscal
EQUADOR	Roberto Carlos Torres Cáceres	Fiscalía General del Estado Agente fiscal de la Unidad Nacional Especializada en Investigación de Ciberdelito
ESPAÑA	Fidel Solera	Fiscalía Provincial de Madrid Fiscal Delegado de Criminalidad Informática y de Tutela Penal de la Igualdad y contra la Discriminación
ESPAÑA	Elvira Tejada	<i>Fiscal de Sala de Criminalidad Informática</i>
GUATEMALA	Jossie Emanuel Valdes Vasquez	Ministerio Público de Guatemala Analista Profesional, Departamento de Análisis de Delitos Informáticos y Cibercrimen
MÉXICO	José Benjamín Oviedo Morales	Fiscalía General de la República Titular de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas
PANAMÁ	Juan Antonio Gomez Castillo	<i>Fiscal Especializado en Delitos Contra la Propiedad Intelectual y Seguridad Informática</i>
PARAGUAI	María Soledad Machuca Vidal	<i>Fiscal Adjunta encargada de la Unidad Especializada de Delitos Informáticos del Ministerio Público</i>
PERÚ	Juan Humberto Flores Cáceres	Ministerio Público Jefe de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público
PORTUGAL	Pedro Verdelho	Diretor do Gabinete Cibercrime
REPÚBLICA DOMINICANA	Andrés Mena	Procuraduría General de la Republica Procurador Fiscal

URUGUAI	Barbara Zapater Erviti	Fiscalia General de la Nación Fiscal Depratamental
CONSELHO DA EUROPA	Oana Tarus	Senior Project Officer <i>Cybercrime Programme Office (C-PROC)</i>
CONSELHO DA EUROPA	Elena Floroiu	<i>Project Assistant</i> <i>Cybercrime Programme Office (C-PROC)</i>
CONSELHO DA EUROPA	Razvan-Daniel Oltean	<i>Project Assistant</i> <i>Cybercrime Programme Office (C-PROC)</i>

ANEXO B

Conferência Internacional sobre a Convenção de Budapeste e Segundo Protocolo

AGENDA

23 de maio de 2023	
14h30	<i>Inscrição dos participantes</i>
14h45	Sessão de abertura Ministério Público Federal do Brasil - Hindenburgo Chateaubriand Filho Conselho da Europa – Pedro Verdelho
15h00	Prepare-se, no Ministério Público e na polícia, para enfrentar o crescimento explosivo do cibercrime e as necessidades de tratamento de provas digitais – Mauricio Fernández (Chile)
15h30	A Convenção de Budapeste e o Segundo Protocolo Adicional – Pedro Verdelho (Portugal)
15h50	Após aderir à Convenção, o que muda para o Brasil? – Fernanda Teixeira Souza Domingos (Brasil)
16h15	<i>Pausa para café</i>
16h30	Cooperação direta com prestadores de serviços no âmbito da Convenção de Budapeste e do Segundo Protocolo Adicional – Elvira Tejada (Espanha)
17h30	Emergência do tráfico de pessoas com utilização das redes de comunicações: as iniciativas da REDTRAM da AIAMP – Marcelo Colombo, por videoconferência (Argentina)
17h45	<i>Fim das atividades do dia</i>

24 de maio de 2023	
9h15	<i>Inscrição dos participantes</i>
09h30	Obtenção de dados dos prestadores de serviços através das autoridades nacionais (artigo 8º do Segundo Protocolo Adicional) – Fidel Solera (Espanha)
10h30	Recolha de dados em situações de emergência: as novas possibilidades do Protocolo – Fidel Solera (Espanha)
11h15	Outras ferramentas de cooperação: videoconferência e equipas conjuntas de investigação – António Segóvia, por videoconferência (Chile)
12h00	<i>Pausa para almoço</i>

14h30	Informações sobre nomes de domínio em cooperação transfronteiriça direta no Protocolo – Elvira Tejada (Espanha)
15h15	O que é a ICANN e porque colabora com a justiça criminal – Carlos Alvarez (ICANN)
16h15	A Resolução de Domínios e Processos de Registo: WHOIS: Como pode a justiça criminal obter acesso à informação de registo de nomes de domínio? – Carlos Alvarez (ICANN)
17h00	A experiência do NIC.br – Demi Getschko (Brasil)
17h30	<i>Encerramento da conferência</i>

ANEXO C

Reunião da *CiberRed*

AGENDA

25 de maio de 2023

09h15	<i>Inscrição dos participantes</i>
09h30	Sessão de abertura Associação Ibero-americana de Ministérios Públicos – Pedro Verdelho Ministério Público Federal do Brasil - Hindenburgo Chateaubriand Filho Conselho da Europa – Oana Tarus
09h45	Estruturas de investigação especializadas na Ibero-América: as que existem e as que são necessárias Discussão aberta entre os participantes Moderação: Fernanda Teixeira Souza Domingos – Brasil
10h30	Implementação do Segundo Protocolo: "autoridades competentes"? Discussão aberta entre os participantes Moderação: Elvira Tejada – Espanha
11h00	Apresentação do Roteiro de Atuação – Criptoativos Apresentação: Thiago Bueno – Brasil
11h45	Investigações relacionadas com criptoativos na Ibero-América Discussão aberta entre os participantes
12h30	Outros assuntos e adoção do relatório da reunião
12h45	<i>Fim da reunião</i>