CiberRed/*CiberRede*

Cibercrime em tempo de pandemia

REUNIÃO EM VIDEOCONFERÊNCIA

18 de setembro de 2020

CONCLUSÕES DA COORDENAÇÃO DA REDE

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA
GABINETE CIBERCRIME

AIAMP
Asociación Ibero Americana de Ministerios Públicos

Cibercrime em tempo de pandemia

REUNIÃO EM VIDEOCONFERÊNCIA

18 de setembro de 2020

CONCLUSÕES DA COORDENAÇÃO DA REDE

A – A REUNIÃO

1. Realizou-se, a 18 de setembro de 2020, uma reunião dos pontos de contacto da CiberRed/*CiberRede*, a Rede Iberoamericana de Ministérios Públicos Especializados em Cibercrime. Esta reunião, que decorreu por meio de videoconferência, incluiu-se nas atividades previstas no programa anual da CiberRed/*CiberRede*, como complemento à reunião anual, que todos os anos se realiza. Sendo muito provavelmente impossível, no contexto de pandemia que se vive, a realização da reunião anual em 2020, esta reunião por videoconferência foi uma alternativa àquela reunião.

2. Participaram 21 representantes de 15 dos países membros da AIAMP[1]. De entre os membros da CiberRed/*CiberRede* apenas não estiveram representados Cuba, Equador, El Salvador, Honduras e México. Quanto à Nicarágua e à Venezuela, ainda não indicaram os seus representantes.
Nesta reunião deram-se as boas-vindas a Andorra, que participou pela primeira vez nos trabalhos da CiberRed/*CiberRede*, convertendo-se no seu vigésimo membro.
Inclui-se no Anexo A a lista de participantes e no Anexo B a agenda da reunião.

3. A CiberRed/*CiberRede* foi constituída na XXIV Assembleia Geral da AIAMP, em Lisboa, em 2016, a qual também decidiu que esta rede seria um fórum para o contacto e o intercâmbio sobre as tendências do cibercrime e a obtenção de prova digital e, portanto, deveria organizar una reunião anual dos seus pontos de contacto. O Ministério Público de Portugal coordena esta rede.

B – O CONTEXTO: PANDEMIA

4. Um dos objetivos da CiberRed/*CiberRede* é o de tornar mais fácil a partilha de informação no âmbito da cibercriminalidade, por intermédio dos pontos de contacto da rede, e que se discutam problemas específicos relacionados com o cibercrime. Este intercâmbio de experiências requere regularidade e continuidade e, para isso, muito pode contribuir a proximidade de relação entre os membros da rede.
Estos propósitos recomendavam a continuidade das atividades da rede, mesmo sendo impossível a reunião física e presencial dos seus pontos de contacto.

5. Por outro lado, havia já ao nível nacional dos distintos países, a impressão de que o tempo de pandemia que se vive trouxe um incremento dos fenómenos delitivos na área do cibercrime. Por todo o lado, no globo, milhões de pessoas estão a trabalhar à distância, nas suas próprias casas, utilizando meios de comunicação remota e acesso a sistemas informáticos de instituições privadas e públicas. Além

[1] Andorra, Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, España, Guatemala, Panamá, Paraguay, Perú, Portugal, República Dominicana y Uruguay.

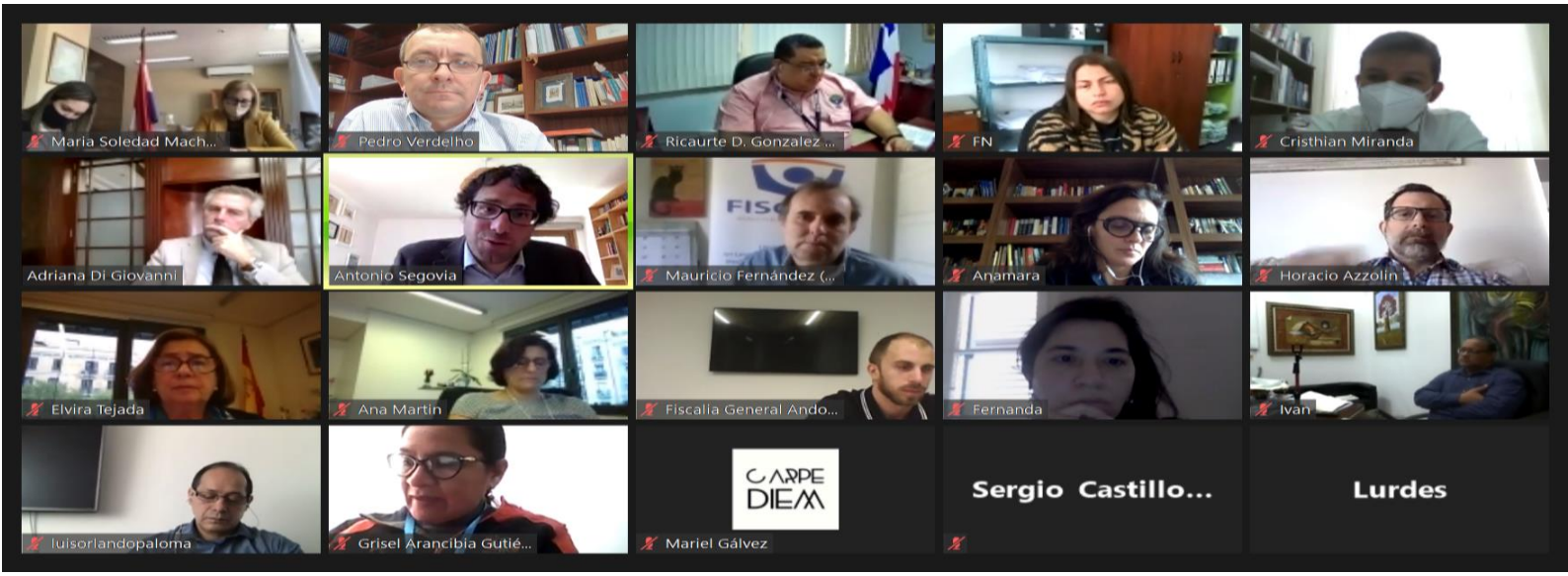
do mais, tudo surgiu muito rapidamente, sem que tivesse havido tempo para a devida preparação, de pessoas e sistemas, para esta nova realidade, a qual, cada dia mais se revela menos passageira que persistente. Portanto, fica também a impressão de que as reflexões que se façam a este propósito não se esgotarão neste tempo. Pelo contrário: muito do que mudou de forma provisória nas nossas atividades, poderá vir a tornar-se definitivo.

6. Também estas razões eram mais do que suficientes para que na CiberRed/*CiberRede* se discutisse o impacto do tempo que se vive no cibercrime ou outras formas de delinquência cometidas através das redes de comunicações, e as consequências que terá no *post* pandemia. Da mesma forma, pareceu muito útil partilhar as tipologias e métodos criminais que, neste período, surgiram e as medidas e estratégias adotadas ao nível interno, pelos diferentes países, para enfrentá-los.

C – CONCLUSÕES DOS DEBATES

C – a) O incremento do cibercrime em geral

7. Uma das conclusões mais presentes nas intervenções dos participantes foi a tendência crescente do cibercrime, em termos estatísticos. Esta tendência não é de agora, mas anotou-se em todos os países um grande incremento deste tipo de fenómeno criminal, depois da eclosão da presente pandemia. Além do mais, também se desenvolveram, de forma muito significativa, outros tipos de criminalidade, de carácter mais tradicional, mas utilizando as redes de comunicação.



C – b) Considerações mais específicas relacionadas com o tempo de pandemia

8. Como ficou dito, para além da constante e crescente tendência geral de incremento do cibercrime, anotou-se um excecional crescimento deste tipo de fenómenos criminais depois da eclosão da pandemia da COVID-19.

Os participantes na reunião referiram, por um lado, o grande aumento do cibercrime *clássico*. Foi o que sucedeu, por exemplo, com o *phishing* ou o *ransomware*. Mas, por outro lado, também foi assinalado o grande desenvolvimento de infrações criminais mais diretamente relacionadas com a pandemia.

Assim, foram assinaladas, por exemplo, muitas burlas relacionadas com produtos falsos ou falsificados (como máscaras, ou outros). Do mesmo modo foram relatados ataques informáticos dirigidos contra

hospitais (com o intuito de obter dados da doença, por exemplo, relacionados com personas famosas) e contra outras instituições públicas.

9. Os participantes descreveram também dois tipos de criminalidade *online* que em muito subiram no tempo de pandemia: os delitos relacionados com pornografia infantil e factos relacionados com a difusão das chamadas *fake news*. No primeiro caso, os indicadores nalguns países (Espanha e Guatemala, por exemplo, mencionaram-no) referiam um altíssimo incremento das participações. Com respeito ao segundo caso, muitos dos participantes revelaram que este fenómeno criminal foi motivo de grande preocupação nos seus respetivos países.

10. Na generalidade dos países participantes, os fenómenos relacionados com as *fake news* não estão especificamente considerados como ilícitos criminais, antes se enquadrando em tipos penais clássicos. A este respeito, a *Fiscalía General del Estado*, de Espanha, elaborou uma nota de "*Análisis del Impacto del COVID19 en la Ciberdelincuencia*", a qual aborda, entre outros, o tema das *fake news*.
Por sua vez, o *Ministério Público Federal*, do Brasil, emitiu um "*Guia de Investigação e Combate à Desinformação na Internet no Contexto da Covid-19*". No Brasil discute-se presentemente um projeto legislativo exatamente neste âmbito. Este projeto legislativo contempla, por exemplo, a obrigação, dos fornecedores de serviço Internet, de comunicarem às autoridades públicas casos desta natureza que venham a identificar.
Assinalou-se que no Panamá existe já uma lei neste domínio, mas apenas dirigida aos direitos dos consumidores – isto é, dirige-se especificamente à publicidade enganadora.
Concluiu-se que a temática das *fake news* correspondeu, talvez, ao único assunto em que, em termos de direito penal substantivo, durante a pandemia, foram anotadas prováveis lacunas legislativas – ou talvez mesmo necessidades legislativas.

C – c) A necessidade crescente de obter prova digital

11. Além da expansão do cibercrime em sentido estrito, anotou-se, como ficou dito, uma grande expansão, também, de outras práticas ilícitas, por meio das redes de comunicação, a qual teve como consequência o grande incremento da necessidade de obtenção de prova digital.
Esta conclusão conduz a diferentes necessidades, em especial no campo da formação de procuradores e de *fiscales*.

C – d) Formação e especialização

12. Autonomizou-se este parágrafo, por corresponder a um tema recorrente nas reuniões da CiberRed/*CiberRede*. Também desta vez se reiterou, de forma insistente, a necessidade de formação dos magistrados e a grande conveniência de especialização nesta área.
Reforçou-se, uma vez mais, que a investigação dos delitos praticados nas redes de comunicações, pela sua complexidade, requere conhecimentos especializados e meios específicos de investigação. Este tipo de requisitos requere, por sua vez, formação e recomenda a criação de unidades especializadas.

C – e) Obtenção de prova digital no estrangeiro

13. Uma das marcas mais importantes dos ilícitos praticados nas redes, ou por via das redes de comunicações, é o seu carácter internacional ou transnacional: em quase todos os casos se requere a

obtenção de prova noutros países, diferentes daquele onde se praticou o crime, ou daquele onde se encontra a vítima.
Esta marca distintiva foi assinalada pelos participantes de uma forma muito forte e com importantes consequências: é que, este tipo de investigações, quase sempre supõe o recurso aos mecanismos de cooperação internacional.
Muitos dos representantes dos diversos países referiram a possibilidade de obter dados, de modo informal, sem recurso aos mecanismos e canais de cooperação internacional, de certos fornecedores de serviços Internet, com sede nos Estados Unidos. Mas não de todos os fornecedores, nem de modo uniforme, uma vez que este processo depende das políticas internas de cada fornecedor de serviços.

14. A verdade é que esta realidade coloca pressão sobre todo o sistema de cooperação internacional: não é sustentável utilizar em todas las investigações (ou quase todas, numa percentagem muito alta), o sistema de cooperação judicial internacional. Este último não está, nem desenhado, nem preparado, para uma tal utilização.
Além disso, tendo como destino, na generalidade dos casos, os Estados Unidos, a experiência de muitos dos participantes revelou que muitas das solicitações de cooperação não são respondidas – diz-se que a competente estrutura dos Estados Unidos para dar sequência a este tipo de solicitações já ultrapassou a sua capacidade de resposta e não consegue dar resposta, a não ser nos casos mais graves ou urgentes.

C – f) Cooperação com a REDCOOP

15. A realidade que acima se descreveu conduz a duas conclusões principais muito relevantes.
Por um lado, neste contexto, é sumamente importante desenvolver modos informais de cooperação entre os países – neste caso, no seio da AIAMP, há diversas possibilidades a explorar, como por exemplo o Acordo de Cooperação Interinstitucional, subscrito na Cidade do México, a 6 de setembro de 2018, por 18 dos Ministérios Públicos membros da AIAMP.
Por outro lado, aos participantes na reunião afigurou-se relevante desenvolver contactos com fornecedores de serviços globais, tendo em vista facilitar procedimentos informais de solicitação de informação.

16. Participou na reunião António Segovia, magistrado do Ministério Público no Chile, coordenador da Rede de Cooperação Penal Internacional da AIAMP (REDCOOP)[2].
Solicitou-se-lhe que apresentasse a REDCOOP e que introduzisse um projeto conjunto que a REDCOOP se propõe desenvolver com a CiberRed/*CiberRede*, de criação de uma listagem de fornecedores de serviços Internet, de modo a facilitar aos magistrados as solicitações de informações no caso concreto. Além desta listagem, o projeto vai desenvolver um guia de boas práticas, respeitantes às solicitações aos fornecedores de serviço.
Este projeto deverá contar com a colaboração de voluntários da CiberRed/*CiberRede*. Além da coordenação da CiberRed/*CiberRede*, voluntariaram-se para colaborar neste projeto as representantes de Espanha e do Brasil.

3 de outubro de 2020

[2] http://www.aiamp.info/index.php/grupos-de-trabajo-aiamp/cooperacion-juridica-internacional

ANEXO A

Cibercrime em tempo de pandemia

LISTA DE PARTICIPANTES

País	Nome	Cargo
ANDORRA	Elisabet Puente Peregrina	*Fiscal Adjunta*
ARGENTINA	Horacio Azzolín	*Unidad Especializada en Ciberdelincuencia*
BOLIVIA	Christian Miranda	
	Grisel Arancibia Gutiérrez	*Jefe de la Unidad de Asuntos Internacionales*
BRASIL	Anamara Osório	*Secretária de Cooperação Internacional Adjunta*
	Fernanda Domingos	*Coordenadora do Grupo de Trabalho sobre Crimes Cibernéticos*
	Neide de Oliveira	*Grupo de Trabalho sobre Crimes Cibernéticos*
CHILE	Antonio Segovia Arancibia	*Director – Unidad de Cooperación Internacional y Extradiciones*
	Mauricio Fernández Montalbán	*Director - Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado*
COLOMBIA	Luis Orlando Paloma Parra	*Fiscal del eje de cibercriminalidad de la Dirección contra las organizaciones criminales*
COSTA RICA	Sergio Castillo Quesada	*Fiscal Auxiliar de la Fiscalía Adjunta Fraudes y Ciberdelincuencia*
ESPAÑA	Ana Maria Martín	*Fiscal de Criminalidad Informática*
	Elvira Tejada	*Fiscal de Sala de Criminalidad Informática*
GUATEMALA	María Elena Galvez Rafael	*Jefa del Departamento de Ciber Delito*
PANAMÁ	Ricaurte González	*Fiscal Superior 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	Maria de Lurdes Lopes	*Assessora do Gabinete da Procuradora-Geral da República*
	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*
URUGUAY	Enrique Rodríguez	*Fiscal Letrado Penal de Montevideo de Delitos económicos y complejos*

ANEXO B

Cibercrime em tempo de pandemia

REUNIÃO EM VIDEOCONFERÊNCIA

18 de setembro de 2019

Uno de los objetivos de CiberRed es que se haga más fácil compartir información en el ámbito de la ciberdelincuencia, por medio de los puntos de contacto de la red, y que se discutan problemas específicos relacionados con el ciberdelito.

En este tiempo difícil de pandemia se señaló un gran aumento de este tipo de fenómenos delictivos, lo que adquirió una dimensión aún mayor ya que hay millones de personas que trabajan a distancia, en su casa, utilizando medios de comunicación remota y acceso a sistemas informáticos, sin que hubiera tiempo para la debida preparación, de personas y sistemas, para esta nueva realidad.

Estas son razones suficientes para que CiberRed discuta el impacto del tiempo que se vive en el ciberdelito u otra delincuencia a través de redes de comunicaciones, y las consecuencias que tendrá en el post pandemia. Así mismo, se ve como muy útil compartir las tipologías y métodos criminales que surgieron y las medidas y estrategias adoptadas a nivel interno por los distintos países, para enfrentarlos.

Um dos objetivos da CiberRede é facilitar a partilha de informações sobre cibercrime, por meio dos pontos de contato da rede, e discutir problemas específicos relacionados com este tipo de delinquência.

Neste difícil período de pandemia, observou-se um grande aumento deste tipo de fenómeno criminoso, que adquire uma dimensão ainda maior por haver milhões de pessoas que trabalham à distância, nas suas casas, utilizando meios de comunicação remotos e acesso a sistemas de informática, sem que tenha havido o tempo suficiente para uma adequada preparação de pessoas e sistemas, para esta nova realidade.

Estes são motivos suficientes para que a CiberRede discuta o impacto do tempo em que vivemos no cibercrime, ou outros crimes praticados por meio das redes de comunicação e as consequências que trará o pós-pandemia. Da mesma forma, será útil partilhar as tipologias e métodos criminosos que surgiram e as medidas e estratégias adotadas internamente pelos diferentes países, para os enfrentar.

REUNIÓN DE VIDEOCONFERENCIA (Zoom)	REUNIÃO EM VIDEOCONFERÊNCIA (Zoom)
16:00 – 19:00 (Madrid) **15:00 – 18:00 (Lisboa)** **11:00 – 14:00 (Brasilia/Buenos Aires)** **10:00 – 13:00 (Santiago)** **09:00 – 12:00 (Lima/Bogotá/México)**	**16:00 – 19:00 (Madrid)** **15:00 – 18:00 (Lisboa)** **11:00 – 14:00 (Brasília/Buenos Aires)** **10:00 – 13:00 (Santiago)** **09:00 – 13:00 (Lima/Bogotá/México)**
Se harán tres presentaciones introductorias (de 10 minutos cada una), seguidas de intervenciones de los puntos de contacto.	Serão feitas três apresentações de introdução (de 10 minutos cada uma), às quais se seguirão intervenções dos pontos de contacto.

TEMAS EN DISCUSIÓN	TEMAS EN DISCUSSÃO
Evolución del ciberdelito en pandemia Medidas y estrategias nacionales introducidas ¿Que cambia en la investigación de delitos digitales? ¿Puede CiberRed apoyar a los fiscales o procuradores nacionales, en investigaciones de otra naturaleza? Cuestiones específicas: *fake news* e otros ilícitos relacionados con la COVID-19	Evolução do cibercrime em pandemia Medidas e estratégias nacionais introduzidas O que muda na investigação de crimes digitais? Pode a CiberRede apoiar os fiscais ou procuradores nacionais em investigações de outra natureza? Questões específicas: *fake news* e outros crimes relacionados com a COVID-19