

CiberRed/CiberRede

Ciberdelito en tiempos de pandemia

REUNIÓN EN VIDEOCONFERENCIA

18 de setiembre de 2020

CONCLUSIONES DE LA COORDINACIÓN DE LA RED

Ciberdelito en tiempos de pandemia

REUNIÓN EN VIDEOCONFERENCIA

18 de setiembre de 2020

CONCLUSIONES DE LA COORDINACIÓN DE LA RED

A - LA REUNIÓN

1. El 18 de septiembre de 2020 se realizó una reunión de los puntos de contacto de CiberRed/CiberRede, la Red Iberoamericana de Ministerios Públicos Especializados en Ciberdelincuencia. Dicha reunión, que ocurrió por medio de videoconferencia, se incluyó en las actividades previstas en el programa anual de CiberRed/CiberRede, como complemento a la reunión anual, que todos los años se celebra. Al ser muy probablemente imposible, en el contexto de pandemia que se vive, la realización de la reunión anual en 2020, esta reunión en videoconferencia fue una alternativa a esa misma reunión.

2. Participaron 21 representantes de 15 de los países de la AIAMP¹. De los miembros de CiberRed/CiberRede apenas no estuvieron representados Cuba, Ecuador, El Salvador, Honduras y México. En cuanto a Nicaragua y Venezuela, todavía no indicaron sus representantes. En esta reunión se dio la bienvenida a Andorra, que participó por vez primera en los trabajos de CiberRed/CiberRede, convirtiéndose en su vigésimo miembro. Se incluye en el Anexo A la lista de participantes y en el Anexo B la agenda de la reunión.

3. CiberRed/CiberRede se constituyó en la XXIV Asamblea General de la AIAMP, en Lisboa, en 2016, la cual también decidió que esta red sería un foro para el contacto y el intercambio sobre las tendencias del ciberdelito y la obtención de evidencia digital y, por lo tanto, debería celebrar una reunión anual de sus puntos de contacto. El Ministerio Público de Portugal coordina esta red.

B - EL CONTEXTO: PANDEMIA

4. Uno de los objetivos de CiberRed/CiberRede 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. Este intercambio de experiencias requiere regularidad y continuidad y para ello mucho puede contribuir la proximidad de relación entre los miembros de la red.

Estos propósitos recomendaban la continuidad de las actividades de la red, aunque siendo imposible la reunión física y presencial de sus puntos de contacto.

5. Por otro lado se tenía, al nivel nacional de los distintos países, la impresión de que el tiempo de pandemia que se vive aportó un incremento de los fenómenos delictivos en el área del ciberdelito. Por todas partes, en el globo, millones de personas están trabajando a distancia, en sus mismas casas,

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

utilizando medios de comunicación y acceso remoto a sistemas informáticos de instituciones privadas y públicas. Además, todo surgió muy pronto, sin que hubiera tiempo para la debida preparación, de personas y sistemas, para esta nueva realidad, la cual cada día más se revela menos pasajera que persistente. Por lo tanto, queda también la impresión de que las reflexiones que se hagan a su propósito no se agotarán en este tiempo. Al contrario: mucho de lo que cambió de forma provisional en nuestras actividades, podrá volverse definitivo.

6. También estas razones eran más que suficientes para que en CiberRed/*CiberRede* se discutiera 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, pareció muy útil compartir las tipologías y métodos criminales que en este periodo surgieron y las medidas y estrategias adoptadas a nivel interno por los distintos países, para enfrentarlos.

C - CONCLUSIONES DE LOS DEBATES

C - a) El incremento del ciberdelito en general

7. Una de las conclusiones más presentes en las intervenciones de los participantes fue la tendencia creciente del ciberdelito, en términos estadísticos. Esta tendencia no es de ahora, pero se anotó en todos los países un grande incremento de este tipo de delito después de la eclosión de la presente pandemia. Además, también se desarrollaron de forma muy significativa otros tipos de criminalidad, de carácter más tradicional, pero utilizando las redes de comunicación.



C - b) Consideraciones más específicas relacionadas con el tiempo de pandemia

8. Como arriba quedó dicho, más allá de la constante y creciente tendencia general de incremento del ciberdelito, se anotó un excepcional crecimiento de este tipo de fenómenos delictivos después de la eclosión de la pandemia de la COVID-19.

Los participantes en la reunión refirieron, por un lado, el gran aumento del ciberdelito *clásico*. Fue lo que pasó, por ejemplo, con el de *phishing* o el *ransomware*. Pero, por otro lado, también fue señalado el gran desarrollo de infracciones criminales más directamente involucradas con la pandemia.

Así, fueron señaladas, por ejemplo, muchas defraudaciones relacionadas con productos falsos o falsificados (como mascarillas, u otros). Del mismo modo fueron relatados ataques informáticos dirigidos a hospitales (con el intuito de obtener datos de la enfermedad, por ejemplo, relacionados con personas famosas) y direccionados a otras instituciones públicas.

9. Los participantes describieron también dos tipos de criminalidad *online* que mucho subieron en el tiempo de pandemia: los delitos relacionados con pornografía de menores y hechos relacionados con la difusión de las llamadas *fake news*. En el primer caso, los indicadores en algunos países (España y Guatemala, por ejemplo, lo mencionaron) referían un altísimo incremento de las denuncias. Con respeto al segundo caso, muchos de los participantes revelaron que este fenómeno criminal fue una gran preocupación de sus respectivos países.

10. En la generalidad de los países participantes, los fenómenos relacionados con las *fake news* no están específicamente considerados como delitos criminales: más bien se enmarcan en tipos penales clásicos. Con respeto a este tema, la Fiscalía General del Estado, de España, elaboró un informe de “Análisis del Impacto del COVID19 en la Ciberdelincuencia”, el cual aborda, entre otros, el tema de las *fake news*.

De su parte, el *Ministério Público Federal*, de Brasil, emitió una “*Guia de Investigação e Combate à Desinformação na Internet no Contexto da Covid-19*”. En Brasil, se discute presentemente un proyecto legislativo en este ámbito. Dicho proyecto legislativo contempla, por ejemplo, la obligación, para los proveedores de servicios Internet, de comunicaren a las autoridades públicas casos de esta naturaleza que vengan a identificar.

Se señaló que en Panamá existe ya una ley en estos dominios, pero apenas dirigido a los derechos de los consumidores – es decir, se dirige más bien a la publicidad engañosa.

Se concluyó que las *fake news* correspondió al único tema en que, en términos de derecho penal sustantivo, en la pandemia, se anotaron probables lagunas legales, o más bien, necesidades legislativas.

C – c) La necesidad creciente de obtener evidencia digital

11. Además de la expansión del ciberdelito en sentido estricto, se anotó, como quedó dicho, una grande expansión, también, de otras prácticas delictivas, con utilización de las redes de comunicación, la cual tuvo como consecuencia el gran incremento de la necesidad de obtención de prueba digital.

Esta conclusión conduce a distintas necesidades, en especial en el campo de capacitación de procuradores y fiscales.

C – d) Capacitación y especialización

12. Se autonomizó este apartado por corresponder a un tema recurrente en las reuniones de CiberRed/CiberRede. También de esta vez se reiteró, de forma insistente, la necesidad de capacitación de los fiscales y la gran conveniencia de especialización en estos temas.

Se reforzó una vez más que la investigación de los delitos practicados en las redes de comunicaciones, debido a su complejidad, requiere conocimientos especializados y medios específicos de investigación. Este tipo de requisitos requieren, a su vez, capacitación y recomiendan la creación de unidades especializadas.

C - e) Obtención de evidencia digital en el extranjero

13. Una de las marcas más importantes de los ilícitos practicados en las redes, o por medio de las redes de comunicaciones, es su carácter internacional o transnacional: en casi todos los casos se requiere la obtención de prueba en otros países, distintos de aquel donde se practicó el crimen, o donde se encuentra la víctima.

Esta marca fue señalada por los participantes de una manera muy fuerte y con importantes consecuencias: es que, este tipo de investigaciones casi siempre supone el recurso a los mecanismos de cooperación internacional.

Muchos de los representantes de los distintos países refirieron la posibilidad de obtener datos, de modo informal, sin recurso a los mecanismos y canales de cooperación internacional, de ciertos proveedores de servicios Internet con sede en los Estados Unidos. Pero no de todos los proveedores, ni de manera uniforme, ya que este proceso depende de las políticas internas de cada proveedor de servicios.

14. La verdad es que esta realidad pone presión sobre todo el sistema de cooperación internacional: no es sustentable utilizar en todas las investigaciones (o casi todas, en un porcentaje muy alto), el sistema de cooperación judicial internacional. Este último no está, ni dibujado, ni preparado, para una tal utilización.

Además, al tener como destino, en la generalidad de los casos, los Estados Unidos, la experiencia de muchos de los participantes reveló que muchas de las solicitudes de cooperación no son contestadas – se dice que la estructura competente en los Estados Unidos para dar secuencia a este tipo de solicitudes ultrapasó ya su capacidad de respuesta y no contesta más que los casos más graves o urgentes.

C - f) Cooperación con REDCOOP

15. La realidad que arriba se describió, ha conducido a dos conclusiones principales muy relevantes.

De un lado, en este contexto es sumamente importante desarrollar modos informales de cooperación entre los países – en este caso, en el seno de la AIAMP hay distintas posibilidades a explorar, como por ejemplo el Acuerdo de Cooperación Interinstitucional, suscrito en la Ciudad de México, el 6 de septiembre de 2018, por 18 de los Ministerios Públicos miembros de la AIAMP.

Del otro lado, a los participantes de la reunión les pareció relevante desarrollar los contactos con los proveedores de servicios globales, con miras a facilitar el proceso informal de solicitudes de información.

16. Participó en la reunión António Segovia, fiscal de Chile y coordinador de la Red de Cooperación Penal Internacional de la AIAMP (REDCOOP)².

Se le solicitó que presentara REDCOOP y que introdujera el proyecto conjunto que REDCOOP se propone desarrollar con CiberRed/CiberRede, de creación de una guía con un listado de proveedores de servicios Internet, de modo a facilitar a los fiscales las solicitudes de información en los casos concretos. Además de esta guía con un listado, el proyecto va a desarrollar una guía de buenas prácticas con respecto a las solicitudes a los proveedores.

Dicho proyecto deberá contar con la colaboración de voluntarios de CiberRed/CiberRede. Además de la coordinación de CiberRed/CiberRede, se han voluntariado para cooperar en este proyecto las representantes de España y Brasil.

3 de octubre de 2020

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

ANEXO A

Ciberdelito en tiempos de pandemia

18 de setiembre de 2019

PARTICIPANTES

País	Nome	Cargo
ANDORRA	Elisabet Puente Peregrina	<i>Fiscal Adjunta</i>
ARGENTINA	Horacio Azzolín	<i>Unidad Especializada en Ciberdelincuencia</i>
BOLIVIA	Christian Miranda	
	Grisel Arancibia Gutiérrez	<i>Jefe de la Unidad de Asuntos Internacionales</i>
BRASIL	Anamara Osório	<i>Secretária de Cooperação Internacional Adjunta</i>
	Fernanda Domingos	<i>Coordenadora do Grupo de Trabalho sobre Crimes Cibernéticos</i>
	Neide de Oliveira	<i>Grupo de Trabalho sobre Crimes Cibernéticos</i>
CHILE	Antonio Segovia Arancibia	<i>Director - Unidad de Cooperación Internacional y Extradiciones</i>
	Mauricio Fernández Montalbán	<i>Director - Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado</i>
COLOMBIA	Luis Orlando Paloma Parra	<i>Fiscal del eje de cibercriminalidad de la Dirección contra las organizaciones criminales</i>
COSTA RICA	Sergio Castillo Quesada	<i>Fiscal Auxiliar de la Fiscalía Adjunta Fraudes y Ciberdelincuencia</i>
ESPAÑA	Ana Maria Martín	<i>Fiscal de Criminalidad Informática</i>
	Elvira Tejada	<i>Fiscal de Sala de Criminalidad Informática</i>
GUATEMALA	María Elena Galvez Rafael	<i>Jefa del Departamento de Ciber Delito</i>
PANAMÁ	Ricaurte González	<i>Fiscal Superior Especializado en Delitos Contra la Propiedad Intelectual y Seguridad Informática</i>
PARAGUAY	María Soledad Machuca Vidal	<i>Fiscal Adjunta encargada de la Unidad Especializada de Delitos Informáticos del Ministerio Público</i>
PERÚ	Ángela Olivia Arévalo Vásquez	<i>Fiscal - Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación</i>
PORTUGAL	Maria de Lurdes Lopes	<i>Assessora do Gabinete da Procuradora-Geral da República</i>
	Pedro Verdelho	<i>Coordenador do Gabinete Cybercrime</i>
REPÚBLICA DOMINICANA	Iván Félix Vargas	<i>Procurador General de Corte, Titular de la Procuraduría Especializada para Delitos de Alta Tecnología</i>
URUGUAY	Enrique Rodríguez	<i>Fiscal Letrado Penal de Montevideo de Delitos económicos y complejos</i>

ANEXO B

Ciberdelito en tiempos de pandemia

REUNIÓN DE VIDEOCONFERENCIA

18 de setiembre 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: <i>fake news</i> 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: <i>fake news</i> e outros crimes relacionados com a COVID-19