**RELATORIO DEL ENCUENTRO DE FISCALES ESPECIALISTAS EN CIBERDELINCUENCIA CELEBRADO EN EL CENTRO DE LA AECID DE LA ANTIGUA (GUATEMALA)**

Durante los días 14 a 18 de octubre de 2019, organizado conjuntamente por la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) y la Fiscalía General del Estado de España, se celebrón en el Centro de Formación de la Cooperación Española en La Antigua (Guatemala) un encuentro de la Red de Fiscales Iberoamericana de Fiscales Especializados en Ciberdelincuencia (CiberRed), constituida en el marco de la AIAMP, que contó con la participación de representantes de Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Panamá, Paraguay, República Dominicana y Uruguay.

Con el objetivo fundamental de fortalecer la CiberRed como herramienta orientada a facilitar y potenciar la cooperación internacional en la lucha contra la ciberdelincuencia, el encuentro se ha desarrollado bajo la forma de Seminario, integrado por diversos talleres de trabajo diseñados con la finalidad de analizar las tipologías delictivas relacionadas con esta forma de criminalidad respecto de las cuales se ha detectado que tienen una mayor incidencia en la Red, así como a tratar las cuestiones técnica y jurídicas más problemáticas relacionadas con la investigación de estas conductas.

**14 de octubre**

La primera jornada comenzó con una exposición sobre los delitos de pornografía infantil y child grooming a cargo de la representante de Paraguay, en la que se puso de manifiesto la importante incidencia que ha tenido el desarrollo tecnológico en este tipo de actividades delictivas causando importante incremento de esta clase de conductas. En el debate que siguió a la presentación del tema, se pusieron de relieve las dificultades para conocer la verdadera entidad de este fenómeno cuya cuantificación resulta muy compleja al tratarse de delitos que normalmente no son investigados a instancia de particulares, sino que, por el contrario, las investigaciones que se realizan tienen su origen en actuaciones iniciadas de oficio por cuerpos policiales en la mayoría de ocasiones a raíz de informaciones que son trasladadas por organismos e instituciones internacionales o cuerpos policiales. Al respecto, se estimó de interés dejar constancia de los datos publicados recientemente por el periódico americano *The New York Times* en el que, tras efectuar una investigación sobre contenidos relacionados con abusos sexuales a menores publicados en la red, se refiere a su aumento exponencial año a año y notoria insuficiencia de los medios necesarios para su erradicación[1].

Concretamente, y en lo que concierne a la problemática asociada a la investigación y actuación penal en materia de pornografía infantil y acoso a menores con fines de carácter sexual, se trató sobre las diferencias de tratamiento en los distintos Estados en lo que se refiere al concepto de pornografía técnica, a la tipificación penal del acceso online a material pornográfico y del acoso a menores o child grooming. Así mismo se analizaron algunos de los problemas concursales que

---

[1] https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html?action=click&module=Top%20Stories&pgtype=Homepage

plantean estas figuras delictivas en relación con el abuso a menores y los delitos contra la intimidad y aspectos relativos a la aplicación de la continuidad delictiva en determinados supuestos.

Otra cuestión objeto de tratamiento fue la relativa a la responsabilidad a personas jurídicas por estas conductas respecto de la cual se extrae la conclusión de que legalmente, salvo en España, no está prevista en prácticamente ninguno de los demás países iberoamericanos si bien en alguno de ellos existen proyectos legislativos en curso con dicho objetivo.

El segundo módulo, estuvo centrado en el tratamiento de los delitos que se dirigen contra bienes personalísimos, comenzó con un repaso de las previsiones al respecto establecidas en la Convención de Budapest, el Convenio de Lanzarote y la Convención de Estambul todas ellas del Consejo de Europa para a continuación analizar, en , la respuesta penal que se está proporcionando desde los distintos ordenamientos jurídicos a los atentados contra la intimidad, el secreto de las comunicaciones y la protección de datos personales a través de las herramientas tecnológicas. Entre otras cuestiones se debatió sobre la tipificación penal de la difusión inconsentida de imágenes de carácter íntimo previamente obtenidas con la anuencia de la víctima y sobre la figura penal del acoso permanente, como derivada del artículo 34 de la Convención de Estambul, que ofrece una solución adecuada a los atentados contra la libertad y seguridad cometidos a través de las Tecnologías de la Información y la comunicación cuando no encuentran encaje en los delitos tradicionales de amenazas o coacciones por falta de los requisitos legales para ello.

Otra cuestión que fue objeto de análisis en relación con estas conductas fue la relativa a la necesidad detectada en algunos países, de tipificar la suplantación de identidad como figura independiente. Una previsión que según se pudo comprobar si que se encuentra contemplada, si bien con matices diversos, en algunos de los ordenamientos jurídicos de los países asistentes, como es el caso de Costa Rica, Colombia, El Salvador y Brasil.

Esta primera jornada concluyó con una sesión de trabajo en la que se trató sobre la incorporación en los ordenamientos jurídicos internos de los tipos penales sobre ataques a sistemas informáticos comprendidos en los artículos 2 a 6 de la Convención de Budapest. A partir de la exposición realizada por el Representante de Chile, acerca del proyecto de Ley sobre el que se está trabajando en el Parlamento de dicho país, se analizaron conjuntamente algunos aspectos de especial interés en esta materia. Entre ellos se trató sobre la respuesta de las legislaciones nacionales frente al *hacking ético*, y en concreto sobre la posible previsión de una cláusula de exención de responsabilidad para estos casos. Al respecto, la mayoría de los países asistentes se mostró contraria a esta posibilidad en el entendimiento de que un acceso no autorizado siempre supone una invasión de la privacidad cuya criminalización no puede quedar condicionada a las razones de justificación que al respecto pudiera alegar el intruso una vez ha sido identificado como presunto responsable de la actividad delictiva.

**15 de octubre**

La segunda jornada de trabajo comenzó con una sesión destinada a analizar las nuevas formas de defraudación que van surgiendo al hilo del desarrollo tecnológico. En relación con ello, el representante de Costa Rica dio cuenta de la regulación existente en este país en el que, junto a las figuras tradicionales de estafa, existe una regulación específica y detallada de las estafas cometidas mediante manipulación informática o artificios técnicos semejante. En el curso del debate suscitado en relación con esta materia, se examinaron otras modalidades de defraudación en las que se combina la manipulación informática con el engaño tradicional, entre

ellas especialmente las fundamentadas en actividades de ingeniería social, phishing, así como la utilización de la simulación de identidad para la obtención fraudulenta de credenciales y claves bancarias.

De la información proporcionada por los asistentes se desprende que modalidades de este tipo de conductas son muy diversas y que presentan diferencias de planificación y ejecución en los distintos países, si bien se detectan problemas comunes en la investigación de estas conductas, así, todos los asistentes coincidieron en la necesidad de establecer protocolos de colaboración con las entidades bancarias para facilitar la obtención de evidencias y de la información relativa a los artificios engañosos utilizados por los autores de estos comportamientos.

En la siguiente sesión de trabajo se trataron las conductas referidas a la difusión de contenidos de odio a través de la Red partiendo de su distinción respecto de otros comportamientos igualmente delictivos y dañinos que se materializan mediante publicaciones en el entorno virtual que inciden contra otros bienes jurídicos como puede ser el honor o la intimidad. Tras analizar las principales iniciativas internacionales para combatir este tipo de conductas, se expuso la regulación en las legislaciones internas de los países asistentes, prestando una especial atención en las dificultades que derivan de la falta de previsión legal en algunas de ellas de determinados motivos de discriminación tales como la homofobia o la aporofobia. Una parte importante de esta sesión de trabajo se dedicó al tratamiento de las medidas orientadas a hacer inaccesibles los contenidos tales como interrupción de la prestación de servicios, retirada de contenidos o el bloqueo.

El segundo tema objeto de tratamiento en esta jornada fue el relativo a los delitos contra la propiedad intelectual e industrial a través de los sistemas informáticos. El representante de Panamá se encargó de su presentación, comenzando por exponer la regulación existente en este país para la protección de estos derechos que incluye la propiedad intelectual e industrial, así como los derechos colectivos de los pueblos indígenas y sus conocimientos tradicionales. En el debate que siguió a esta exposición, los asistentes compartieron información sobre la regulación de esta materia en sus legislaciones internas, que llevan a la conclusión de que en esta materia se detectan diferencias entre los distintos países en las formas de lesión de estos derechos y por ende en los tipos penales previstos para su protección.

La última sesión de trabajo se destinó a tratamiento de la investigación criminal de la cibedelincuencia y, en especial, a la investigación en fuentes abiertas de estas conductas. En el transcurso de esta actividad, que corrió a cargo de representantes de cuerpos especializados de la Policía Nacional y Guardia Civil de España, se informó a los asistentes de las posibilidades de investigación que existen en fuentes abiertas de internet, sus ventajas y desventajas, los distintos entornos de la red en que se llevan a cabo estas investigaciones y las nuevas herramientas y técnicas de investigación que se emplean en esta clase de investigaciones y sus posibilidades. Las cuestiones que fueron planteadas por los asistentes a ambos ponentes en el transcurso de su intervención evidenciaron la importancia de contar con una capacitación técnica complementaria de la jurídica para poder afrontar estas investigaciones con garantías de éxito.

**16 de octubre**

La tercera jornada de trabajo, ya plenamente inmersos en la temática relacionada con la investigación tecnológica, comenzó por una sesión de trabajo dedicada al análisis del marco legal establecido en la Convención sobre Ciberdelincuencia del Consejo de Europa. Tras efectuar un breve repaso a los avances en la armonización normativa respecto a la definición de tipos

penales, se examinaron las principales herramientas de investigación que se diseñan en la Convención de Budapest del Consejo de Europa. Concretamente, la preservación de datos, la orden de entrega por terceros de datos informáticos almacenados el registro de sistemas y dispositivos informáticos, así como la confiscación e incautación de evidencias electrónicas. Al respecto se suscitó un debate especialmente interesante en referencia al acceso transnacional a los datos informáticos y a la obtención de datos de abonado de Proveedores de Servicio radicados en otros Estados.

El representante de República Dominicana efectuó una presentación en la que examinó en profundidad la regulación de la preservación de datos a nivel nacional y transnacional desde la perspectiva de la regulación efectuada por la Convención de Budapest. En el transcurso de su exposición se detuvo especialmente en el análisis de los diversos requisitos exigibles en atención a las diferentes clases de dato que pueden ser objeto de reclamación: abonados, tráfico o contenido. Al hilo de esta cuestión también se analizó la doctrina del TJUE en relación con el acceso a los datos conservados y la problemática que plantea en el curso d e las investigaciones (8/4/14, 21/12/16 y 2/10/2018)

Las sesiones de tarde de esta tercera jornada estuvieron dedicadas a reflexionar sobre los nuevos entornos a los que se enfrenta la investigación tecnológica determinados por la propia evolución de los dispositivos y tecnologías a través de las cuales se realizan las conductas delictivas. Los representantes de cuerpos especializados en la investigación policial analizaron algunas de las técnicas más novedosas de la investigación tecnológica empleadas en la interceptación de comunicaciones y el registro remoto de dispositivos. En relación con el primero, se pusieron de relieve los retos que se plantean al investigador con el cifrado generalizado de las comunicaciones, especialmente las que se producen de punto a punto, así como las posibilidades tecnológicas actuales que pueden posibilitar la interceptación de los contenidos antes de su cifrado o cuando se ha producido su descifrado por el receptor de la comunicación. En lo que concierne al registro de dispositivos informáticos se trató sobre las nuevas formas de almacenamiento de información, muy condicionadas por la propia evolución de los dispositivos de comunicación y en especial por la potencialidad de los smartphones para generar información y almacenarla en la nube o en entornos virtuales. Una parte de la intervención se destinó a informar a los asistentes de las nuevas herramientas que se han ido creando con la finalidad de posibilitar la investigación de estos nuevos sistemas de almacenamiento.

**17 de octubre**

Esta jornadacomenzó por una sesión de trabajo destinada a tratar sobre la orden de presentación de datos y la cooperación de los Proveedores de Servicio. Los representantes de Uruguay y Brasil se encargaron de presentar el tema a partir de su regulación en la legislación interna en sus respectivos países. En el debate que siguió a ambas presentaciones los asistentes se refirieron al distinto tratamiento dado en sus normativas internas en relación con la incorporación de datos al proceso en atención a su diferente categoría – abonados, tráfico o contenido – pudiendo apreciar un distinto nivel de exigencia en los diferentes países sobre la necesidad o no de autorización judicial para el acceso a los datos. Así mismo, los asistentes, de forma prácticamente unánime, se refirieron a la problemática que plantea la obtención de dato almacenados por Proveedores de Servicios que no están sujetos a la jurisdicción interna del país donde se desarrolla la investigación. Si bien en algunos casos se regula el sometimiento de estos Proveedores por el mero hecho de prestar servicios a usuarios de la nación en estos casos surgen problemas para la efectividad o ejecutoriedad de las órdenes de obtención de datos dadas por

la Autoridad Judicial, en relación los acuerdos de colaboración con los Proveedores de Servicio se revelan como una buena práctica que contribuye a solventar gran parte de estos problemas.

La mañana concluyó con el análisis de algunas de las técnicas de investigación más empleadas frente a la ciberdelincuencia, realizado en una mesa redonda en la que se combinaron los aspectos jurídicos y técnicos de la figura del agente encubierto y los equipos conjuntos de investigación como herramienta eficaz para la investigación de delitos que afectan al territorio de dos o más Estados. Partiendo de la regulación proporcionada al agente encubierto online en la legislación española tras la reforma en la Ley Procesal efectuada en éste país en el año 2015, se debatió sobre la regulación de esta figura en los demás países, apreciando que muchos de ellos carecen de una regulación específica si bien se emplea esta figura aplicando la normativa del agente encubierto físico. Entre otras cuestiones se analizaron los distintos niveles de infiltración a que puede dar lugar la investigación policial en red y las garantías exigibles en cada uno de ellos, la problemática de la introducción de archivos ilícitos en la red y su control judicial, así como los problemas que pueden plantear algunos supuestos en relación con la provocación delictiva.

La sesión concluyó con una exposición relativa a las ventajas que ofrecen los equipos conjuntos de investigación frente a esta forma de delincuencia netamente transfronteriza a partir del análisis de algunos casos prácticos donde se había empleado esta herramienta. También se analizó su tratamiento en la normativa internacional y en las legislaciones internas.

Las sesiones de tarde estuvieron destinadas a analizar la importancia de la cooperación internacional en la investigación de la ciberdelincuencia y la necesidad de contar con herramientas que permitan agilizar y hacer más eficaz la asistencia internacional. En una mesa redonda integrada por los representantes de Guatemala, Chile, Colombia y Uruguay, se expusieron las normas que regulan la cooperación internacional en las respectivas legislaciones destacando la preocupación por las dificultades que plantea el acceso a la evidencia alojada en terceros países y la falta de colaboración de los Proveedores de Servicio. Por el representante de Chile se analizó la importancia que ha tenido para este país su incorporación a la Convención de Budapest, a partir de la cual en la Fiscalía han apreciado mayores posibilidades de cooperación con otros países, y ha supuesto un plus en la negociación de acuerdo con los Proveedores de Servicios. En el transcurso del debate, se puso de relieve la preocupación por la rigidez de algunos de los instrumentos de cooperación internacional actualmente existentes que chocan con la urgencia que suele acompañar a la solicitud de cooperación para la obtención de la evidencia electrónica dada la naturaleza de esta. Se insistió en la necesidad de contar con herramientas de cooperación más ágiles y eficaces y en el valor que puede aportar la CiberRed a este fin. También se destacó la importancia de que los receptores de las solicitudes de auxilio relacionadas con los ciberdelitos cuenten con conocimientos especializados que les permitan una actuación y ejecución de la solicitud adecuada y con la salvaguarda de las evidencias con todas las garantías.

La última sesión de trabajo se dedicó a tratar sobre el establecimiento de sistemas internos de especialización de los Ministerios Públicos como la mejor forma de asegurar una respuesta eficaz contra la ciberdelincuencia y a la importancia de la CiberRed como herramienta para facilitar la cooperación internacional y como entorno para el intercambio de experiencias y nuevas prácticas que contribuya al éxito de estas investigaciones en las que se aprecia que todos los países se enfrentan a similares problemas. Se estudiaron las conclusiones de la última reunión de la CiberRed, celebrada en Chile el pasado mes de junio, avalando todas y cada una de ellas y se insistió en la necesidad de solicitar de la IberRed que posibilite el uso de Iber@ como canal

de comunicación seguro de la Red en el que se instale una biblioteca virtual en la que compartir normativa, iniciativas internas, casos prácticos...etc. También se trató sobre la posibilidad de crear una guía práctica o un protocolo de actuación de la Red.

**18 de octubre**

Esta última jornada de trabajo se dedicó al análisis de todo lo trabajado en los días previos y a la redacción por parte de todos los asistentes de las Conclusiones alcanzadas en relación con ello.

La actividad concluyó con la entrega de diplomas a los asistentes y clausura de la actividad.

La Antigua (Guatemala)
18 de octubre de 2019

Ana Mª Martín Martín de la Escalera