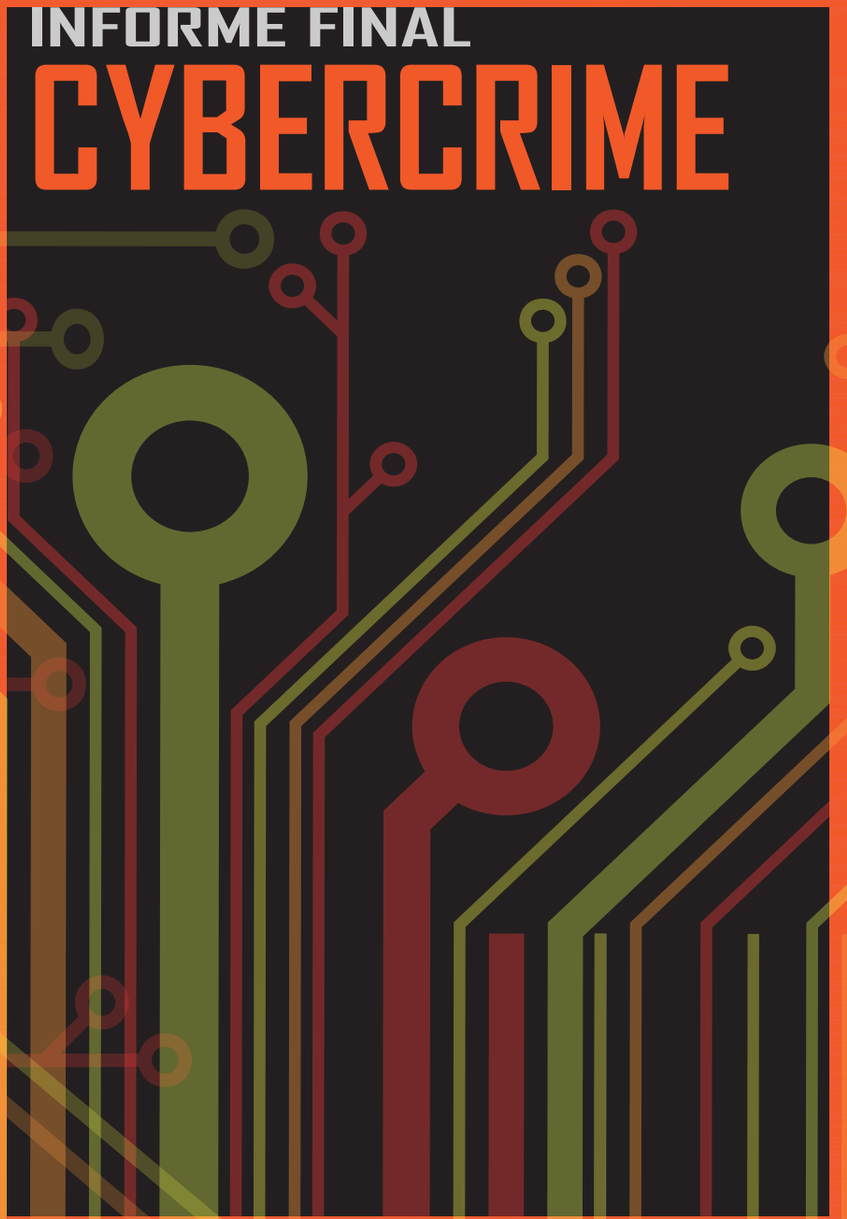
Ministerio Público Fiscal
de la Ciudad Autónoma de Buenos Aires

INFORME FINAL
CYBERCRIME



EQUIPO ESPECIALIZADO EN DELITOS INFORMATICOS DE LA CABA

EQUIPO ESPECIALIZADO EN DELITOS INFORMÁTICOS

Equipo de trabajo

Daniela Dupuy

Tomás Vaccarezza

Mariana Kiefer

Catalina Neme

PRESENTACIÓN

El 15 de noviembre de 2012, la Fiscalía General de la CABA dictó la Resolución 501/12, a través de la cual, creó como prueba piloto por el término de un año, el Equipo Fiscal Especializado en Delitos y Contravenciones Informáticas, que actúa con competencia única en toda la Ciudad Autónoma de Buenos Aires, con el fin de investigar los delitos informáticos propiamente dichos, y aquellos que se cometen a través de internet que por su complejidad en la investigación o su dificultad en individualizar a los autores, merecen un tratamiento especializado.

POLICIALES › DELITOS INFORMÁTICOS

Una fiscalía dedicada a los delitos informáticos

Funciona como prueba piloto en la Ciudad. No hay ninguna nacional.

COMPARTIR 0 Email 5 Twittear 9 Me gusta 100 Compartir +1 0 Compartir 0 Share 8

ETIQUETAS Delitos informáticos

03/02/13

Por lo pronto se trata de una experiencia piloto de un año. Pero lo cierto es que desde el 15 de noviembre último en Buenos Aires funciona **la primera fiscalía especializada en Delitos Informáticos**. Esta unidad de investigaciones – hasta ahora, única en su tipo en el país– fue creada por el Ministerio Público de la Ciudad. Su tarea: investigar casos que van desde el daño informático hasta la producción y distribución de material pedófilo en la red, pasando por el "bullying" (acoso a través de las redes sociales, principalmente) o amenazas, siempre por medio de un soporte tecnológico.

Como la fiscalía especializada –a cargo de Daniela Dupuy– pertenece a la Justicia de la Ciudad, los hechos en los que puede intervenir son limitados. Por ejemplo, no les corresponde investigar casos de defraudaciones, estafas o abusos de menores facilitados por medio de Internet.

"Los avances tecnológicos han introducido **nuevos riesgos en la sociedad,** pues su desarrollo aumentó significativamente e incidió en la relaciones humanas", evaluó el fiscal general porteño Germán Garavano en los fundamentos de su resolución 501/12, por la que se creó la fiscalía. La integran cuatro abogados que trabajan tanto con la Policía Federal como con la Metropolitana y el Cuerpo de Investigaciones Judiciales (Policía Judicial de la Ciudad).

"Hoy por hoy los casos que más nos preocupan –por su características y por lo que crecen– son **los de pornografía infantil**. En general las investigaciones se inician por pedidos de fuerzas internacionales, como Interpol, que localizaron en Buenos Aires a los usuarios", explicaron a **Clarín** en la fiscalía especializada.

Ante este panorama, uno de los principales proyectos para 2013 "es hacer campañas en los colegios, sobre todo hablar con los chicos para explicarles los riesgos que corren", señalaron.

Diario Clarín 3 de febrero de 2013

Lo cierto es que este equipo fiscal trabajó en una propuesta en la que se fundamentaron los motivos por los que consideraba importante la creación de una fiscalía encargada de investigar este tipo de delitos; como ser el aumento progresivo del número de ingreso de conductas penales vinculadas a la nueva tecnología; la forma de investigación muy diferente a las investigaciones tradicionales, ya que requieren de herramientas informáticas específicas para detectar, recolectar y preservar la evidencia digital; la necesidad de que exista una unidad de actuación fiscal para aplicar nuevos protocolos de trabajo que permitan arribar a resultados eficientes, entre otros.

Ello, sumado a una serie de objetivos que nos propusimos, cuyo análisis de evolución y resultados se detallarán en el presente informe, hizo que el Fiscal General nos confiara este desafío, y creemos estar trabajando muy fuerte para lograr que se concrete un proyecto más de los tantos obtenidos durante esta gestión.

DESAFÍOS PARA LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS

Considero que existen, al menos, cuatro temas centrales sobre los que se requiere trabajar profundamente, y sobre los que se apoyaron los objetivos propuestos por este equipo fiscal.

En primer lugar, es fundamental adaptar las normas de fondo a la utilización de herramientas informáticas para cometer delitos, debiendo reconocer la velocidad de la innovación de las redes.

Desde una **perspectiva nacional**, la sanción de la **ley 26.388** incluyó una serie de delitos informáticos en el Código Penal, actualizando nuestro sistema penal.

Sin embargo resta mucho por hacer. Es cierto, o al menos discutible, que algunas de estas modalidades delictivas quizás no requieran de la creación de un tipo penal específico para incriminarlas, y que se pueden subsumir en conductas ya contempladas en nuestro Código Penal.

Sin embargo, debemos tener en cuenta que nuestra ley penal es de la década del 20', y entonces ampara bienes jurídicos que responden a otra era tecnológica.

Pero si partimos de la base que no existe delito sin ley previa, de acuerdo a lo establecido en el art. 18 de la Constitución Nacional y, que no es posible la interpretación penal por analogía, la realidad es que hoy, las conductas llevadas a cabo a través de medios tecnológicos, dejan obsoletas muchas normas jurídicas, al punto de tener que declarar atípicas conductas que requieren de una protección penal.

Un ejemplo de ello, es la sanción de la Cámara de Diputados del 11/9/2013 que aprueba la conducta de Grooming y la incorpora al art. 125ter del CP., tema que desarrollaré en los próximos ítems.

Desde el **ámbito internacional**, hoy hablar de delitos en Internet sin un enfoque de estas características es imposible, toda vez que las redes atraviesan el planeta y no hay fronteras.

Los países más industrializados entendieron que era necesario armonizar sus leyes y establecer medios técnicos y procedimientos de cooperación para combatir los delitos cometidos por Internet.

Esa fue la génesis de la Convención de Ciberdelito y de otros instrumentos internacionales, tales como Protocolo adicional contra la Xenofobia en Internet; Protocolo relativo a la venta de niños que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño.

Todo ello ha demostrado que la localidad del derecho debía ceder frente a la globalidad de la red, incluso en un ámbito como el derecho penal y procesal que siempre estuvo tan ligado a la soberanía.

Los estados miembros del Consejo de Europa y los otros estados firmantes del **Convenio de Budapest** –redactado en el año 2001- habían tenido experiencia en casos transnacionales y cometidos a través de internet, y coincidieron en la necesidad de llevar a cabo una política penal común destinada a prevenir la criminalidad mediante internet, a través de una legislación apropiada de cada estado.

Si bien Argentina y el resto de los países de la región no suscribieron inicialmente el Convenio por no ser parte del Consejo de Europa, nada impide que adoptemos sus ideas y sugerencias como forma de mejorar nuestras leyes.

Nuestro país recibió la invitación a participar en las Conferencias Anuales sobre Ciberdelito en Estrasburgo- Francia.

En segundo lugar, es fundamental reformar las normas procesales. No es lo mismo la recolección de la evidencia digital que de la recolección de prueba física a la que se refiere la mayoría de los códigos de procedimiento.

Existen una serie de temas susceptibles, al menos, de ser discutidos para analizar la posibilidad de introducirlos en los códigos, como por ejemplo, el agente encubierto; la solicitud de preservación y obtención de datos, la validez de la prueba obtenida en otro país, el registro de cosas físicas versus el registro de datos; la posibilidad de aplicar un software judicial a distancia, cuestiones de competencia, utilización de tecnología de cifrado, etc.

Muchas de estas cuestiones son abordadas y discutidas cuando analizamos el alcance de investigación de los delitos informáticos, y cada una de ellas, presenta diferentes aristas que requieren ser expresamente tratadas en las leyes de forma.

En tercer lugar, es muy importante fortalecer los mecanismos de **Cooperación Internacional**.

En muchos casos los procesos de transferencia de datos afectan a varios países. Cuando el delincuente no se encuentra en el mismo lugar que la víctima, la investigación requiere la cooperación entre las autoridades competentes de todos los países que resulten afectados.

El principio de soberanía nacional no permite que un país lleve a cabo investigaciones dentro del territorio de otro país sin el expreso permiso de las autoridades locales. Por lo tanto, las investigaciones deben realizarse con el apoyo de las autoridades de todos los países implicados.

En la mayoría de los casos se dispone de un breve tiempo para que la investigación sea exitosa. Sin embargo el clásico régimen de asistencia mutua presenta evidentes dificultades cuando se trata de investigaciones de ciberdelitos, pues los procedimientos son muy largos.

En cuarto lugar, es fundamental estrechar lazos con **los proveedores de servicio de Internet** (PSI). Ellos nos suministrarán información vital para la investigación.

El problema es que los PSI no están regidos por reglamentación alguna que los obligue a otorgar esa información al investigador.

Sin embargo, y mientras ello ocurra, es conveniente que aquellos sepan qué información necesitamos en cada caso concreto, y el tiempo en que nos hará falta; y los PSI nos notificarán si es posible otorgarnos lo que solicitamos y, en caso positivo, cómo debemos efectuar dichos requerimientos.

OBJETIVOS PROPUESTOS Y OBJETIVOS ALCANZADOS

Sobre la base de los puntos señalados en el acápite anterior, elaboramos los objetivos primarios para que el Equipo Especializado comience a funcionar, los cuales serán enumerados a continuación con el consiguiente resultado.

Investigar delitos informáticos en los que la justicia de la CABA resulte competente y en los delitos cometidos mediante la utilización de medios informáticos

Competencia

Fue necesario delimitar el ámbito en que se concretaría la actividad asignada a la fiscalía especializada, toda vez que el desarrollo de las tecnologías de información hace que sea cada vez mayor el número de bienes jurídicos objeto de protección penal; existiendo conductas ilícitas que se llevan a cabo a través de las ventajas que ofrecen las nuevas tendencias informáticas y consecuentemente presentan dificultades a los efectos de su investigación.

Sin embargo, esta circunstancia no debe llevarnos a considerar que cualquier conducta delictiva en cuya ejecución se utilicen dichas tecnologías, o bien delitos comunes que requieran evidencia digital, deba incluirse en la categoría que nos ocupa, pues ello daría lugar a una desnaturalización del concepto e incluso a un desbordamiento del propio planteamiento de la especialización. Fue preciso delimitar entonces el objeto de actividad en esta área de trabajo con el fin de otorgarle mayor operatividad y eficacia; de forma tal que únicamente alcance su competencia cuando la utilización de dichas tecnologías resulte ser determinante en el desarrollo de la actividad delictiva, o dicha circunstancia implique una mayor complejidad de investigación del hecho e identificación de sus responsables.

No resulta sencillo definir el marco objetivo de actividad de esta especialidad, toda vez que la rápida evolución de la ciencia y tecnología, aconsejan no limitar en un catálogo cerrado los tipos penales susceptibles de encuadrarse en esta categoría de criminalidad informática, ya que es previsible la aparición próxima de nuevas formas de delincuencia o nuevos medios de comisión de delitos ya tipificados, en los que el elemento determinante sea también la utilización de los medios informáticos.

Las circunstancias señaladas determinaron que el catálogo inicial de delitos de criminalidad informática, que a continuación se expone estructurado en tres categorías, quede necesariamente abierto y su inclusión será evaluada previa y oportunamente por la Secretaría de Política Criminal.

Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos

-Delito de daño: La ley 26388 incorpora como segundo párrafo del art. 183 CP *"En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño"*

Daño agravado: La ley 26388 agrega dos nuevas agravantes al art. 184 CP: 5) *"ejecutarlo en archivos, registros, bibliotecas, ….o en datos, documentos, programas o sistemas informáticos públicos"; 6) "ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público"*

Delitos en los que la actividad criminal se ejecuta a través de los medios informáticos

El delito de pornografía infantil: art. 128 CP sanciona al que *produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que quien organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil, y de tenencia con fines de distribución. Será reprimido con prisión de 4 meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.*
Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años.
Delito de amenazas (art.149bis CP) cometidos a través de medios informáticos y/o de comunicación cuando la importancia y complejidad del hecho revista la necesidad de un tratamiento especial.

Suministro de material pornográfico: El art 62 CC sanciona a quien suministra o permite a una persona menor de 18 años el acceso a material pornográfico.

Estadísticas de casos ingresados

GRÁFICO 1: Ingreso de casos período 15 de noviembre de 2012 a octubre 2013

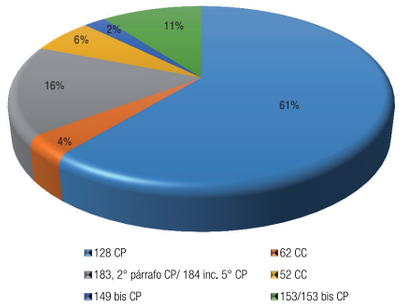
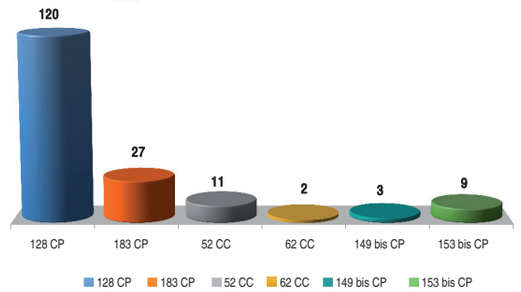


GRÁFICO 2: Resolución de casos

GRÁFICO 3: Casos en trámite al día de la fecha



Como podemos apreciar en el **gráfico 1,** el **67%** del universo de casos informáticos ingresados desde la fecha de creación de la Fiscalía Especializada hasta el presente es de **pornografía infantil.**

Son casos cuya investigación demanda tiempo por circunstancias ajenas a la fiscalía (respuestas de los proveedores de servicio de internet (ISP), peritajes complejos, información que solicitamos a otros países, etc.), No obstante ello, se ha logrado resolver en este período el porcentaje de casos que refleja el **gráfico 2**, con una **alta calidad de resolución.**

Hoy se encuentran en plena **etapa de investigación 172 casos**, discriminados según el delito, tal como lo muestra el **gráfico 3.**

Particularidades de las investigaciones informáticas

Con relación a los casos informáticos que ingresan a la fiscalía, es necesario efectuar algunas particularidades que surgen en la investigación de cada uno de ellos:

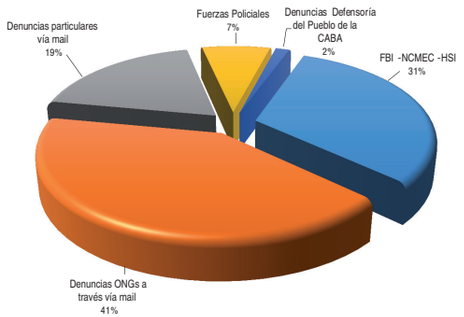
Pornografía infantil

La complejidad para llevar a cabo este tipo de investigaciones implica un análisis pormenorizado de cada medida adoptada por la fiscalía para arribar a un resultado positivo. Son de destacar varias cuestiones que reflejan dicha complejidad y en base a ello, la adopción de ciertas medidas y sus consecuentes resultados

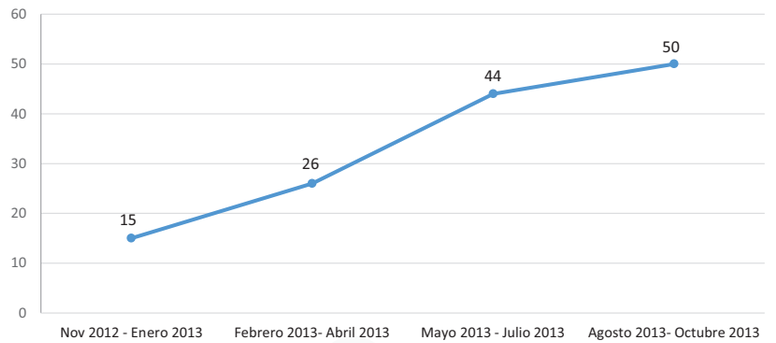
Ingresos: Las denuncias por pornografía infantil son iniciadas por:

1. FBI , quienes reciben la información a través del National Center for Missing and Exploited Children (NCMEC)
2. Homland Security Investigation
3. Particulares a través de comisarías, web mail, Unidades Receptoras de Denuncias
4. Herramienta Google AdWords:
5. ONG'S
6. Defensoría del Pueblo
7. Google AdWords, se ingresa en el buscador ciertas palabras como "delitos informáticos", "pornografía", "como denunciar bullyng". La página arroja como primer resultado de la búsqueda y en un cuadro destacado el link *fiscalías.gob.ar/denuncias-online*, donde se pueden radicar denuncias por pornografía infantil a través de web mail. Desde su puesta en funcionamiento y por un período de tres meses, se incrementó notablemente el número de denuncias de pornografía infantil, en un **69%** -ver gráfico de ingreso progresivo trimestral-
8. Fuerzas policiales de distintos países que advierten en sus investigaciones que se estaría cometiendo el ilícito en la República Argentina, las cuales llegan aquí a través de Interpol.

Modo de ingreso de casos de pornografía infantil



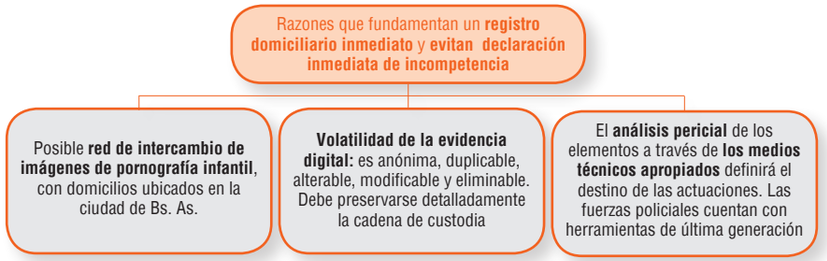
Ingreso progresivo trimestral de casos de Pornografía Infantil

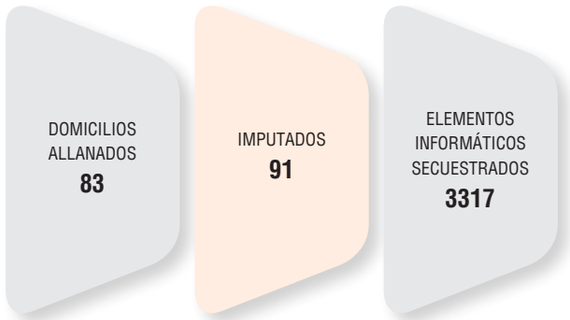


De acuerdo a los ingresos evidenciados en los últimos trimestres, conforme se desprende del gráfico de ingreso progresivo de casos, se estima que el número de **ingreso de casos** solo de pornografía infantil de aquí a un año, al menos, **se duplicará.**

Allanamientos de pedofilia: La lógica de estas investigaciones hace fundamental el registro de los domicilios de los eventuales imputados para asegurar la evidencia digital y consecuentemente realizar el correspondiente informe forense. Lo expuesto llevo a que, en el transcurso del año, **se solicitaron 124 allanamientos,** los que fueron otorgados en su mayoría; y se secuestraron gran cantidad dispositivos informáticos.

En muchos casos, en que los domicilios de las IP se encuentran fuera del ámbito local, entendemos que debe hacerse el análisis forense PREVIO a decidir sobre la posible incompetencia toda vez que el resultado del peritaje podría confirmar que no son conductas autónomas y que estamos en presencia de una red de pedofilia que amerita ser investigada en su conjunto por una cuestión de eficacia procesal.





Grooming

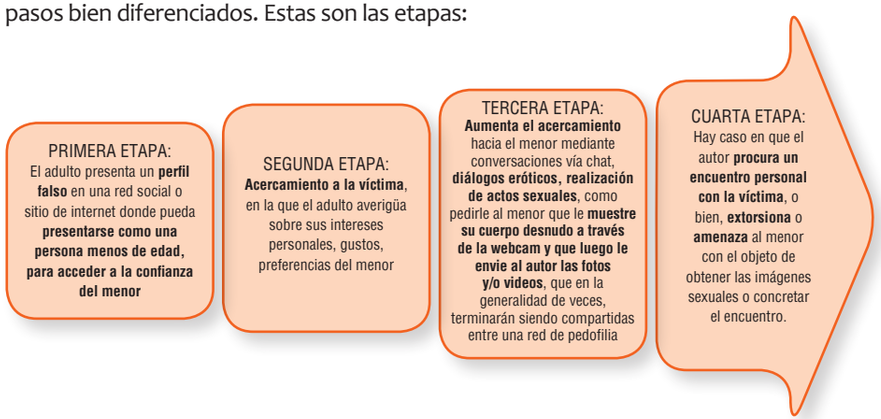
De las investigaciones de pornografía infantil es frecuente que se desprenda, del análisis de la evidencia digital secuestrada, modalidades que podrían considerarse casos de Grooming, conducta recién aprobada por la Cámara de Senadores para ser incorporada como delito autónomo en nuestro Código Penal.

Ello es importante tenerlo en cuenta pues, seguramente, será competente la justicia local, toda vez que es un tipo penal creado con posterioridad al Convenio de Transferencia y, además, sería difícil escindir dichas modalidades de los casos de pedofilia.

Lo expuesto impactará consecuentemente en el número de casos investigados.

Entendemos por *grooming* las conductas consistentes en el acoso o seducción de un adulto a un menor, en muchos casos haciéndose pasar por un menor de edad, con el fin de obtener algún tipo de gratificación sexual, o imágenes sexuales del menor, o bien, como antesala de un posible encuentro personal con la víctima en aras de abusar de él.

De un análisis de las conductas investigadas surge, del contenido de las conversaciones vía chat o e-mail, un patrón común de acción de los autores, con pasos bien diferenciados. Estas son las etapas:



Amenazas. Hostigamiento. Bullying

Se entiende por Bullying al maltrato físico y/o psicológico deliberado y constante que recibe un niño por parte de otro u otros, en forma personal o bien a través de las redes sociales.

Estas conductas se materializan en posibles amenazas, hostigamientos y, en algunos casos, en delitos más graves.

A través de la herramienta Google AdWord se determinó una búsqueda significativa de la sociedad para conocer cómo y dónde se denuncian este tipo de conductas.

La tendencia de un grupo equivalente a 19.633 búsquedas está dado en el ingreso reiterado de las palabras "como denunciar bullying" o "bullying escolar", o "cyberbullying".

Al analizar el historial de palabras claves, en el que se pueden ver reflejadas las búsquedas que se hicieron en google, se concluye que este grupo se orienta hacia una problemática entre niños en las escuelas.

El problema consiste en que, al ingresar estas eventuales modalidades delictivas al ámbito penal, nos encontramos, en la mayoría de los casos, con que los autores son menores de edad, por lo tanto son inimputables.

Esto requiere de un nuevo análisis en cuanto a la necesidad de trabajar profundamente en la prevención de las conductas para evitar el ingreso al sistema penal.

En consecuencia, la Fiscalía Especializada en Delitos Informáticos, con el apoyo

invaluable de la Secretaría de Acceso a la Justicia del Ministerio Público Fiscal de la CABA, junto con el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la CABA, Ministerio de Educación de la Nación y Consejo de Niños, Niñas y Adolescentes, se encuentran trabajando fuertemente en la organización de una Campaña de concientización, formación y prevención para los colegios de la ciudad, sobre una estructura aplicada al Programa "Fiscales a la Escuela", con el fin de informar sobre las diferencias entre derecho a la intimidad y a la privacidad, sobre las consecuencias jurídicas que pueden acarrear la comisión de tales conductas, orientar a los padres, a los docentes y a las víctimas de Bullying, y brindar las herramientas necesarias para prevenir.

Los resultados y agenda del proyecto se señalarán en el punto II.-g)

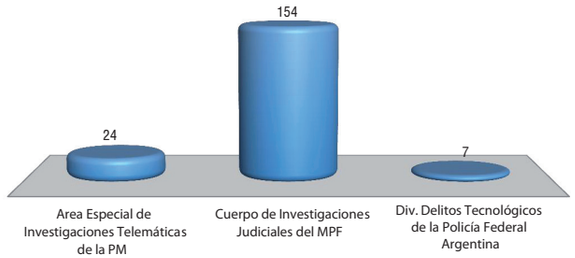
Acceso ilegítimo a sistemas informáticos: necesidad de inclusión en la Resolución FG 501/12

Con la aprobación de la "Ley de Delitos Informáticos" - ley nro. 26.388, publicada en el Boletín Oficial el 25-06-08-, se incorporó la figura del art. 153 bis del CP que prevé: "*Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un* ***sistema o dato informático de acceso restringido****. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*". Si bien este delito, no se encuentra previsto en los Convenios de Traspaso de Competencias Penales y Contravencionales de la Justicia Nacional Ordinaria a la Ciudad Autónoma de Buenos Aires –Leyes Nacionales nro. 25.752 y 26.357, Leyes de la Ciudad nro. 597 y 2257-, ello se debe a que el mismo fue sancionado con posterioridad a la celebración de los Convenios antes aludidos. Así, y tal como indicara el Sr. Fiscal General -Dr. Germán Garavano- en la Resolución FG 152/08, entendemos que la competencia para intervenir en la investigación de este delito corresponde a la Ciudad Autónoma de Buenos Aires.

En esta línea, y en virtud de que la conducta prevista en el art. 153 bis del CP tiene por objeto "un sistema o dato informático de acceso restringido", sostenemos que el mismo debería ser incluido en las competencias exclusivas asignadas por resolución FG 501/12 al Equipo Especializado en Delitos Informáticos.

Coordinar criterios y estrategias de investigación adecuadas con las unidades especiales de las distintas fuerzas de seguridad especializadas –Policía Federal Argentina y Policía Metropolitana, Gendarmería Nacional- y el Cuerpo de Investigaciones Judiciales

Intervenciones a Fuerzas Policiales en casos de pornografía infantil



Para investigar delitos informáticos es fundamental el trabajo coordinado y continuo con las fuerzas de investigación y policiales.

En esta línea, la fiscalía especial trabaja intensamente con el Cuerpo de Investigaciones Judiciales; área Telemática de la Policía Metropolitana; y Delitos Tecnológicos de la Policía Federal Argentina.

Las tres fuerzas están dotadas de excelente personal técnico y, en mayor o menor medida, poseen herramientas de última generación para obtener, preservar, y peritar todos los soportes informáticos secuestrados en los allanamientos.

Se llevan a cabo reuniones periódicas entre el Equipo Especializado y cada una de las fuerzas.

La primera de ellas, apenas recibido el caso, consiste en diseñar en forma conjunta la estrategia de investigación para cada caso en concreto, a través de intercambio de opiniones técnicas y jurídicas para asegurarnos el éxito y eficiencia de la investigación.

El resto de las reuniones son de seguimiento del trámite de los casos, acordando nuevas medidas a raíz del resultado de las primariamente adoptadas.

Elaboración de Protocolos de actuación que faciliten y unifiquen los criterios de actuación en la investigación de los hechos delictivos que requieran para su eficiente investigación de la obtención de evidencia digital.

El equipo de trabajo ha comenzado a trabajar, a raíz de los resultados obtenidos de las mejores prácticas procesales aplicadas para investigar los delitos informáticos, en la elaboración de Protocolos de Actuación para cada uno de los tipos penales que se encuentran dentro de la órbita informática.

Si bien, ello facilita y esquematiza el cuantioso trámite existente, en especial con relación a la pornografía infantil, es fundamental analizar cada caso en concreto para ajustar dicho Protocolo de Actuación y adoptar las medidas necesarias.

Promover institucionalmente Convenios de Cooperación con el sector privado a los fines del cumplimiento eficiente de los requerimientos de la justicia de los distintos proveedores de servicio y las distintas cámaras que los nuclean

Los datos de los abonados son esenciales para determinar la ubicación de las IP obtenidas por los técnicos.

En esa misma línea, la preservación de los datos de tráfico y la obtención de los datos de contenidos que se requiere a las empresas proveedoras de servicio, son sumamente necesarias y su respuesta rápida, conforman un eslabón fundamental para el éxito de la investigación.

El problema de la falta de regulación y de legislación acerca de la obligación de las empresas proveedoras de servicio ante los requerimientos judiciales hace que aquellas respondan cuando quieren, como quieren y lo que quieren, con las lógicas consecuencias negativas q ello trae aparejado para una investigación de este tipo.

Esa realidad nos llevó a efectuar reuniones de trabajo con los diferentes representantes de aquellas para acordar y discutir los términos de los requerimientos, qué solicitar, cómo hacerlo, los requisitos formales que exige cada empresa, qué pueden darnos y qué no es posible, el tiempo que demanda la respuesta, hacerles saber la información que necesitamos para la investigación y en el tiempo preciso, generar enlaces con algún representante; etc.

Algunas de las empresas son de Argentina, otras son extranjeras pero tienen su sede en la Argentina, y otras ni siquiera están instaladas en el nuestro país lo cual dificulta aún más sus respuestas a nuestros requerimientos.

Lo expuesto nos llevó a fortalecer los vínculos con representantes de las siguientes empresas:

a. Telefónica / Movistar
b. Telecom
c. Cablevisión / Fibertel
d. Mercado Libre
e. Google
f. Amcham Argentina: Cámara de comercio de Estados Unidos en la Argentina.

Sin perjuicio del intercambio de opiniones y necesidades acerca de los requerimientos judiciales, nos encontramos en tratativas para generar para el próximo año, un Taller de Capacitación para fiscales e investigadores.

Coordinar con el Centro de Formación Judicial el entrenamiento del equipo fiscal asignado en relación con la investigación de los delitos cometidos a través de internet y la realización de cursos básicos de actuación para todos los integrantes del MP.

La capacitación de los fiscales, jueces y defensores, y de quienes integran las respectivas dependencias, resulta fundamental para entender la lógica en la investigación de los delitos informáticos y en la actualización constante que la problemática requiere.

En consecuencia, hemos participado activamente en la organización de las siguientes actividades de capacitación, cuyo desarrollo se encuentra en el ANEXO I:

Jornadas en que la Fiscalía Especializada participó de la organización

- 4tas Jornadas de Actualización del Poder Judicial de la Ciudad Autónoma de Buenos Aires –Noviembre 2012. "La evidencia digital en el proceso penal moderno"
- Delitos Informáticos y Evidencia Digital en el Proceso Penal –Abril 2013. "Nuevas Técnicas de Investigación para los Delitos informáticos"
- Conferencia Regional IACA para América Latina –Mayo 2013. "Ciber amenazas y Cooperación Internacional"
- Jornadas de Actualización del Poder Judicial de la CABA. Noviembre de 2013. "Investigación de delitos cometidos a través de Internet"

Jornadas como disertante

- Taller "Por una mejor regulación de Internet en Argentina: fortaleciendo estrategias y experiencias comparadas en América Latina" –Agosto 2013. Universidad de Palermo
- Jornadas Nacionales de Asistencia a la Víctima –Septiembre 2013. Posadas-Misiones. "Las víctimas de grooming y bullying"
- Seminario de Pruebas Informáticas –Septiembre 2013. Universidad de San Andrés
- IX Seminario Internacional sobre Delitos Tecnológicos y sus Técnicas de Investigación –Octubre 2013. Policía Federal Argentina
- VII Jornada de Derecho y Delitos Informáticos –octubre 2013. Universidad del CEMA

Generar intercambios de experiencias y cooperación entre las diferentes provincias y CABA en materia de delincuencia informática

Se han llevado a cabo reuniones con fiscales de Argentina; Estados Unidos; España; Brasil; y Paraguay, con el objetivo de garantizar la mejor actuación judicial y la aplicación de criterios similares en la interpretación y aplicación de las normas, y facilitar una adecuada coordinación con las fuerzas policiales en aquellas investigaciones informáticas en las que la actividad delictiva se desarrolla y/o produce sus efectos en diversos lugares geográficos del país.

En igual sentido, se ha intercambiado experiencias acerca de procedimientos en curso, análisis y valoración de los problemas jurídicos, y diferentes legislaciones vigentes en cada país.

Establecer vínculos con otros organismos para coordinar aspectos de utilidad para el desarrollo de la investigación de delitos informáticos

Se han llevado a cabo encuentros de trabajo con diferentes organismos que aportan, desde sus diferentes áreas de funcionamiento, experiencias enriquecedoras y de utilidad para nuestro desempeño, y la posibilidad de concretar, en forma conjunta, acuerdos que redundan en un beneficio para la comunidad; como ser: talleres en colegios; facilitación para canalizar denuncias de hechos que podrían configurar delitos de nuestra competencia; etc.

Algunos de ellos son: el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la CABA; Ministerio de Educación de la Nación; Consejo Niños, Niñas y Adolescentes; Ministerio de Justicia de la Nación; entre otros.

Promover la organización y celebración de actividades formativas con países con experiencia en la investigación especializada de criminalidad informática.

Sin perjuicio del contacto informal que hemos mantenido con fiscales especializados en ciberdelitos de diferentes países, tal como señalé en el punto anterior, uno de los objetivos que resta cumplimentar es organizar actividades y talleres de entrenamiento e intercambio de experiencias entre fiscales de la región y provenientes de otros países, invitando a participar al resto de fiscales que investiguen delitos comunes, toda vez que aumenta día a día la injerencia de la utilización de soportes informáticos para cometer todo tipo de delito.

PÁGINA WEB DE LA FISCALÍA ESPECIALIZADA EN DELITOS INFORMÁTICOS

Con ayuda invaluable del Área de Tecnología de Fiscalía General, hemos logrado poner en funcionamiento una página web, a la cual puede ingresarse independientemente ***www.delitosinformaticos.fiscalias.gob.ar***, o bien, a través de la página del Ministerio Publico fiscal de la CABA.

El principal objetivo es hacer conocer nuestro trabajo diario; informar las novedades de la jurisprudencia local, nacional e internacional en la materia; incluir artículos de editorial de profesionales en delitos informáticos; promover la participación en las jornadas de capacitación que se brindan en las diferentes universidades e instituciones; etc.

La sociedad cuenta con la facilidad de acceder a efectuar denuncias de delitos informáticos desde la página web de la Fiscalía Especializada.

CASOS TESTIGO

OPERACIONES "HISTORIA" Y "PUREZA 2": PEDOFILIA

HISTORIA
+
PUREZA 2

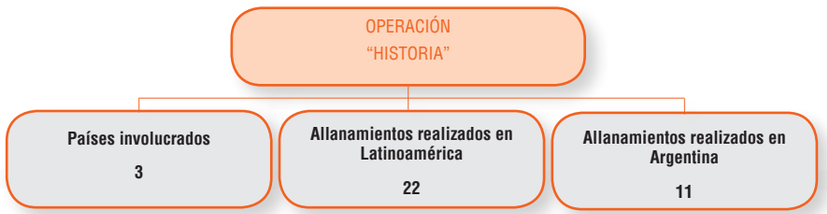
Países involucrados	Allanamientos realizados	Elementos informáticos incautados
9	109	6066

OPERACIÓN "HISTORIA"

Se inicia la investigación a raíz de las actuaciones remitidas por Interpol España, a través de la División Delitos Tecnológicos de la PFA, de las que surge que un ciudadano español **enviaba y recibía e-mails de distintos contactos, los que versaban sobre el intercambio de archivos donde aparecían menores de edad realizando actividades sexuales explícitas o representaciones de sus partes íntimas con fines sexuales. Se verificó un total de ochenta y nueve (89) usuarios de Ecuador, Costa Rica, Colombia, Chile, Argentina y España, que intercambiaron con el imputado esta clase de material.** Específicamente, en el caso de Argentina, se advirtieron **doce (12) usuarios a lo largo de todo el país.**

Realizada la correspondiente investigación e identificados los domicilios desde los que se enviaron los correos en cuestión y, desde los que se accedió a las cuentas investigadas, se coordinaron allanamientos simultáneos en toda Latinoamérica para el día 6 de agosto de 2013. De esto, se colige que en la conducta antes indicada, **intervienen varios actores que conforman un núcleo cerrado en todas las etapas de elaboración, distribución y ofrecimiento de las imágenes y/o videos en cuestión,** lo que demanda una rápida intervención conjunta para el éxito de las investigaciones.

Los allanamientos realizados fueron sumamente exitosos, lográndose secuestrar gran cantidad de elementos informáticos que actualmente están siendo peritados, a fin de determinar e identificar a los participantes de esta red de intercambio, como así también la responsabilidad de cada uno de ellos. (ver resultados en Anexo II).



LA RAZÓN.es

Jueves, 24 Octubre 2013. Actualizado a las 22:50h

LA RAZÓN.es

OPINIÓN
Alfonso Ussía
Una buena edad

EL TIEMPO
Madrid
Máx. 19ºC
Mín. 13ºC

PORTADA OPINIÓN ESPAÑA INTERNACIONAL ECONOMÍA SOCIEDAD RELIGIÓN DEPORTES MOTOR CULTURA TOROS EDICIONES GENTE

SE HABLA DE

SOCIEDAD

Cien detenidos en España y Latinoamérica en una operación contra la pornografía infantil

Imagen de Archivo Efe

16 de agosto de 2013, 13:49h

Efe. Madrid.

La operación contra la pornografía infantil en Internet en la que han participado la Policía Nacional y la Guardia Civil se ha saldado con más de cien detenidos e imputados en diversos países de Latinoamérica y España, con registros en localidades de Alicante y Valencia, han informado a Efe fuentes de la investigación.

Esta actuación contra el cibercrimen se enmarca en un operativo internacional coordinado por Interpol en el que han participado, además, policías de Argentina, Brasil, Colombia, Costa Rica, Chile, Ecuador, Uruguay y Venezuela.

Los diferentes cuerpos de seguridad han participado en esta operación para luchar contra la distribución y tenencia de material pornográfico infantil a través de una conocida red de intercambio de archivos P2P.

Desarrollada en dos fases, en la primera, denominada "Pureza 2", las fuerzas de seguridad han practicado 87 registros en esos ocho países y en España, y han detenido e imputado a 78 personas.

En esta primera fase, la Policía Nacional ha arrestado en España a nueve personas e imputado a otras tres y ha registrado distintos domicilios desde los que se habían realizado las conexiones: tres en Madrid, dos en A Coruña y uno en Granada, Orense, Las Palmas, Málaga, Sevilla, Barcelona y Valencia.

Por su parte, la Guardia Civil ha logrado identificar en el ámbito de su demarcación territorial nueve domicilios en distintas localidades de las provincias de Barcelona, Valencia, Oviedo, Alicante, Zaragoza y Madrid.

Los agentes del Instituto Armado han practicado cinco detenciones y han imputado a dos personas.

La segunda fase, denominada "Historia", ha tenido lugar en Argentina, Costa Rica y España, con un total de 22 registros y otros tantos detenidos e imputados.

La Guardia Civil ha participado en esta fase y ha arrestado a tres personas en Soria, Sevilla y Madrid.

Además, en las dos fases en España, se han intervenido 116 discos duros, 18 lápices de memoria y cerca de 900 CD y DVD en los que había gran cantidad de archivos de pornografía infantil, entre otros efectos.

Los investigadores estiman que puede haber varios miles de archivos de contenido pedófilo, con imágenes de gran dureza.

Todos ellos serán minuciosamente analizados para determinar la posible existencia de un delito de producción de material pornográfico infantil, abusos sexuales sobre menores por parte de alguno de los implicados o la existencia de conexiones con otros pederastas que interactúen en la red.

VÍDEOS

NOTICIA 8 ANTENA 3 DEPORTE 6

Multitudinario adiós a Manolo Escobar en su capilla ardiente

Una mujer muere atropellada al señalizar un accidente de tráfico

Los Príncipes de Asturias ya están en Oviedo

ENCUESTA

¿Cree que la huelga convocada en la educación tiene carácter político o son motivos exclusivamente educativos?

- Tiene carácter político
- Tiene carácter educativo

LO MÁS

MÁS RECIENTES MÁS LEÍDO

1 Defender es divertido

2 BFA y Bankia rescinden su contrato con Moody's que dejará de calificarlas

3 «El descubrimiento del bosón deja muchas preguntas sin responder»

4 El Gobierno hará una revisión «global» de la política de I+D+i en 2014

5 Carga policial contra un grupo de radicales frente al Ministerio de Educación en Madrid

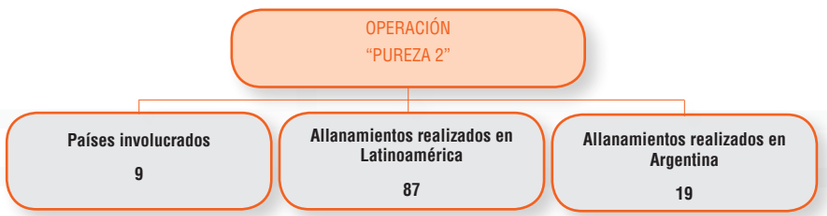
Diario La Razón 24 de octubre de 2013

OPERACIÓN "PUREZA 2"

Se inicia en virtud de la información brindada por la Policía de Investigaciones de Chile, país en el que se implementó una base de datos que registra archivos de video de índole pornográfico infantil, que han sido incautados en diferentes investigaciones. A través de un sistema informático, se identifican distintos usuarios de programas en redes P2P –como son los programas Ares, Edonkey, Emule, etc.- que se encuentren compartiendo los archivos en cuestión. De esta forma, el personal policial chileno **detectó gran cantidad de usuarios con conexiones en Uruguay, España, Ecuador, Costa Rica, Venezuela, Perú, Colombia, Chile, Argentina y Brasil, que realizaron estas acciones de almacenamiento, distribución y/o descarga de material pornográfico infantil, dentro de los cuales se identificó a veintitrés (23) usuarios con conexión en nuestro país.**

Luego de realizar una exhaustiva investigación, tanto en este país como en el resto de Latinoamérica, se acordó realizar el día 9 de agosto de 2013 el registro domiciliario de los lugares desde los que se habría facilitado material pornográfico infantil a través de redes P2P. Los numerosos casos de pornografía infantil como así también los estudios realizados al respecto, demuestran que estas conductas se dan en el marco de una comunidad, lo que ameritaba la acción coordinada y conjunta de los países involucrados.

Los registros domiciliarios efectuados fueron altamente exitosos, provocando gran repercusión en los medios internacionales ya que se logró secuestrar gran cantidad de elementos informáticos que, posteriormente y luego de efectuarse las pericias que correspondan, nos permitirán identificar a los posibles miembros de una red de intercambio de pornografía infantil y el grado de responsabilidad de cada uno de ellos. (ver resultados en Anexo I).



Clarín.com
POLICIALES

Home Política Mundo Sociedad Ciudades Policiales Cartas Blogs Deportes

DESCUBRÍ LO FÁCIL
>QUE ES COMPRAR EN NETSHOES <

POLICIALES · DELITOS INFORMÁTICOS

Detienen a 30 personas acusadas de integrar una red de pedófilos

Hicieron 19 allanamientos y en uno de los domicilios descubrieron una especie de estudio de grabación de las imágenes pornográficas con menores de edad.

COMPARTIR

12/08/13 - 19:42

Treinta personas acusadas de formar parte de una organización de pedófilos fueron detenidas durante 19 allanamientos realizados por la policía en la Capital Federal y en el interior del país.

Fuentes policiales explicaron hoy que durante los operativos los investigadores hallaron CD's y computadoras con fotos y películas pornográficas de menores de edad y hasta descubrieron un estudio de grabación donde supuestamente se filmaban las imágenes.

ETIQUETA
Delitos informáticos, Pornografía infantil, pedofilia

Los acusados, todos mayores de edad, fueron arrestados durante 19 allanamientos realizados en la última semana por la Policía Federal en la Ciudad de Buenos Aires y en las provincias de Tucumán, Córdoba, Entre Ríos, Santa Fe y Buenos Aires.

Los voceros explicaron que los procedimientos se realizaron en el marco de la denominada operación internacional "Pureza 2", dirigida por Interpol, de la cual participan policías de Uruguay, Ecuador, España, Perú, Colombia, Costa Rica, Brasil y Chile, en cuyos países también fueron arrestadas personas acusadas de formar parte de la misma organización de pedófilos.

Las fuentes indicaron que en uno de los allanamientos, concretados en La Plata, los detectives hallaron más de 1.500 CD's y computadoras con pornografía infantil.

Diario Clarín 12 de agosto de 2013

ABC.es | INTERNACIONAL

ACTUALIDAD DEPORTES CULTURA VIAJAR GENTE&ESTILO TV VIDEO SALUD BLOGS HEMEROTECA SERVICIOS TECNOLOGÍA

Lo mejor del séptimo arte MuyCine

INTERNACIONAL / PRODUCCIÓN Y DISTRIBUCIÓN

Treinta detenidos en Argentina en un operación contra la pornografía infantil

AGENCIAS / MADRID | Día 12/08/2013 - 20:50h

- Se trata de una campaña internacional con ramificaciones en otros paises latinoamericanos y España

Fuerzas de seguridad argentinas han detenido a treinta personas, en una operación internacional contra una banda dedicada a la producción y distribución de pornografía infantil en Internet con ramificaciones en otros paises latinoamericanos y España. Los treinta detenidos en la operación, llevado a cabo conjuntamente por Interpol Argentina y la Policía Federal argentina en seis provincias del país, son todos mayores de edad y de nacionalidad argentina, según informaron fuentes judiciales y del Ministerio de Seguridad a la agencia oficial Télam.

Estas detenciones forman parte de una operación internacional contra la pornografía infantil denominado 'Pureza 2', en la que, además de Argentina, también participan Uruguay, España, Ecuador, Costa Rica, Venezuela, Perú, Colombia, Chile y Brasil. Las fuerzas de seguridad efectuaron 19 registros en la capital de Argentina y en las provincias de Buenos Aires, Santa Fe (este), Entre Ríos (este), Tucumán (norte) y Córdoba (centro).

En uno de ellos, en la ciudad de La Plata, a unos 60 kilómetros al sureste de Buenos Aires, los agentes encontraron 1.500 discos compactos con material pornográfico, 20 discos externos, cámaras de vídeo, ordenadores y servidores que apuntan a que esta localización funcionaba como punto de distribución. En San Miguel de Tucumán, a 1.311 kilómetros al noroeste de la capital argentina, los detenidos contaban con un domicilio en el que se descubrió una habitación oculta, a la que se accedía a través de un falso techo, provista de equipamiento para la producción de películas caseras. Una vivienda situada en la ciudad de Córdoba, a 700 kilómetros al noroeste de Buenos Aires, habría servido presuntamente como centro para la edición de vídeos de contenido sexual.

Sigue ABC.es en...
Facebook Twitter Tuenti

Últimos Posts

EL TALÓN DE AMÉRICA
Las urnas sin CFK

ARCHIVO DE INDIAS
Limpia, pica y da esplendor

TRAS UN BIOMBO CHINO

MISSING CHILDREN: PRISIÓN PREVENTIVA POR PEDOFILIA

En día 29 de septiembre de 2013 la Fiscalía Especializada en Delitos Informáticos de la CABA, solicito la prisión preventiva de un imputado por pedofilia a raíz de un allanamiento llevado a cabo el viernes 28 de septiembre por la Policía Metropolitana, en cual se secuestraron diversidad de soportes informáticos, fotografías de muy menores de edad (aproximadamente dos o tres años) con contenido sexual, y la presencia en lugar de una menor de 13 años que por su actitud y nerviosismo y estado de angustia se investigará si fue víctima de esta conducta delictiva o de otra subsumida en algún otro tipo penal más grave.

En el mismo allanamiento el imputado quedo detenido y se efectivizo la audiencia de solicitud de prisión preventiva.

La fiscalía investiga el caso desde hace un año con el fin de determinar, a raíz de información suministrada por el FBI a través de una denuncia que le hiciera Missing Children, si el posible autor, conforma una red de pedófilos que intercambia, facilitan, comercializan y /o producen material pornográfico con menores de edad involucrados, hecho subsumido en el art. 128 del CP

La fiscalía, con la adhesión de la Asesora Tutela Adjunta, Dra. Ángeles Burundarena, solicitó la prisión preventiva del imputado por el término de un mes en el que se desarrollaría el peritaje ordenado, fundada en el posible entorpecimiento para la investigación que podría representar que el imputado quedara libre, no solamente por la posibilidad de acceder a la nube y borrar, alterar o modificar datos y prueba que nos impida llegar a otros posibles integrantes de la red, sino también, por las eventuales actitudes que podría tomar para con su hermana menor de edad con quien convive en el mismo hogar.

Así, la titular a cargo del Juzgado en lo Penal n° 9, Dra. María Laura Martinez Vega, dictó la Prisión Preventiva del imputado y resolvió en la misma audiencia extraer testimonios a la justicia nacional para que investigue posibles conductas de abuso sexual o corrupción de menores.

La Sala III, tras apelación de la defensa, decidió, casi veinte días después de la audiencia, dejar en libertad al imputado en un fallo carente de análisis de los argumentos de la fiscalía, sobre los cuales había basado su decisión la Sra. juez de grado.

INTERPOL ALEMANIA: CONDENA POR PORNOGRAFÍA INFANTIL

Con fecha 12 de enero de 2009 se recibió requerimiento de INTERPOL WIESBADEN, Alemania, de Klaus Bayer, Jefe de la OCN, informando que a partir del 3 de julio de 2008, la Oficina de Policía Criminal de Baden- Wuettemberg (Alemania), inició búsquedas de archivos de pornografía infantil en la red eDonkey 2000, las que

revelaron que varios clientes ofrecían copias de archivos de pornografía infantil, las que habían sido previamente guardadas en esa sede policial. De esta forma, fue identificado el link **ed2k** de los archivos en cuestión, y por medio de ese link se inició un pedido de allanamiento a la red eDonkey 2000. Dicho pedido de allanamiento, arrojó una lista de usuarios (identificados a través de los números de IP), **quienes almacenaron completamente estos archivos con los contenidos de pornografía infantil y los pusieron a disposición para ser descargados de la comunidad eDonkey 2000, encontrándose también incluidos los usuarios mencionados del cliente emule.** De esta forma, la policía alemana guardó un log de datos de aquéllos que ofrecieron este archivo (direcciones de IP y las estampillas de hora) que constituyó el punto de partida de nuestra investigación.

Arribada aquí dicha información, con la colaboración de la División Delitos Informáticos de la Policía Federal Argentina, se inició investigación a fin de obtener los datos de ubicación de los IP suministrados por Alemania, identificando las empresas prestadoras de servicios de Internet de los IP en cuestión, como así también los usuarios de los mismos.

Con fecha 4 de mayo de 2011 se recibió el informe final realizado por la División Delitos Informáticos de la PFA, del que surgen gran cantidad de domicilios en los cuales las tareas de investigación encomendadas arrojaron resultados positivos. En razón de ello, a solicitud de este Equipo Fiscal, el Juzgado que correspondía intervenir en el caso libró la totalidad de 41 órdenes de allanamiento, algunas de ellas en esta Ciudad y otras en el interior del país.

Los allanamientos llevados a cabo en el marco de la investigación dieron resultado positivo ya que se logró secuestrar gran cantidad de elementos informáticos los que fueron peritados por el Cuerpo de Investigaciones Judiciales en forma conjunta con la División Delitos Tecnológicos de la P.F.A., en virtud de las cuales se pudo establecer que en su mayoría contenían instalados programas del tipo P2P, que utilizaban para intercambiar imágenes donde se exhibían a menores de edad dedicados a actividades sexuales explícitas o representaciones de sus partes genitales con fines predominantemente sexuales.

Luego de confeccionados los informes labrados en relación al material secuestrado, se solicitó la incompetencia en relación a las conductas en infracción al artículo 128 del C.P.N que fueron llevadas a cabo en extraña jurisdicción. Por último, se continuó la investigación en esta sede respecto de los usuarios con asiento en esta ciudad.

INCOMING: A JUICIO POR PEDOFILIA

Respecto de uno de los usuarios investigados, el informe pericial arrojó que la carpeta "incoming" se halla instalada en el directorio raíz en la carpeta /Users/ale/Downloads/eMule/incoming, en la cual se encontraron ubicados veintiocho (28) con contenido pornográfico. Se estableció también que los archivos en cuestión fueron colocados en la mencionada carpeta el día 3 de junio de 2012 y a disposición de todos los usuarios del programa emule. Dicho requerimiento no fue cuestionado por la Defensa y el caso se encuentra en la etapa oral del proceso.

CONDENA: AVENIMIENTO POR PEDOFILIA

En relación a otros de los casos verificados en la Ciudad Autónoma de Buenos Aires, se celebró con el imputado y su defensa un acuerdo de avenimiento en los términos establecidos por el artículo 266 del CPPCABA. Dicho acuerdo fue convalidado por el Juzgado y en definitiva **se condenó al imputado a la pena la pena principal de dos años (2) de prisión** la que deberá ser dejada en suspenso, en virtud de la carencia de antecedentes penales por su parte. Asimismo, se dispuso que deberá someterse a las siguientes reglas de conducta, de conformidad con lo previsto por el artículo 27 bis del CP.., a saber: 1) Fijar residencia y someterse al cuidado de un Patronato y; 2) Someterse a un tratamiento psicológico, previo informe labrado por el Cuerpo de Medicina Legal, que acredite su necesidad y eficacia (inc. 6). Todo ello, por el plazo de duración de la condena solicitada.

DIRECT TV: DAÑO INFORMÁTICO

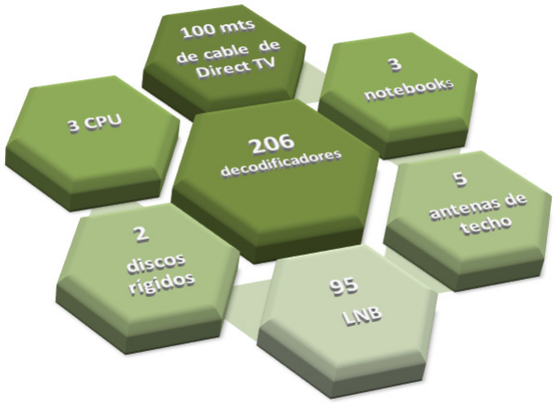
La firma Direct TV denunció la existencia y comercialización ilegal de tarjetas bloqueadoras denominadas "Bloker" o "tarjeteros", las cuales son utilizadas para reemplazar a las Smart cards que provee la empresa, las que al ser insertadas en los decodificadores, poseen los códigos de decodificación de las señales emitidas vía satélite, accediendo de esta manera a la programación brindada por la empresa.

Las Smart Cards originales actúan bajo la misma modalidad que un chip telefónico, es decir, que se puede solicitar telefónicamente el servicio de televisión satelital cuya duración variará de acuerdo al monto cargado. Cabe destacar que la principal función del "bloker" ilegal consiste en no permitir la baja del servicio una vez consumido el crédito cargado legalmente con anterioridad por el usuario.

Este Equipo fiscal consideró que la conducta constituía, al menos, el delito de daño informático previsto en el artículo 183, segundo párrafo del Código Penal de la Nación; al no permitir el ingreso del comando u orden que envía el sistema de la empresa prestadora del servicio una vez concluido el período abonado anticipadamente. Es decir, se impide con esta maniobra que el sistema de gestión de Direct TV cumpla con la misión para la cual fue concebido, quedando de esta manera acreditado el daño.

Mediante la realización de tareas de investigación, se determinó la existencia de un domicilio donde habría depositado el material utilizado para el armado de los decodificadores y la identidad de los posibles imputados, lo que ameritó que se realizara un allanamiento en el lugar, el cual dio como resultado el secuestro de cantidad de material relacionado con la comisión del delito que aquí se investiga y; una vez finalizado el peritaje ordenado, la Fiscalía podrá evaluar la eventual existencia de conductas más graves, como contrabando y defraudación.

Elementos secuestrados en allanamiento del caso Direct TV



IMPORTANTE ESTUDIO JURÍDICO: DAÑO INFORMÁTICO

El caso se inició en virtud de la denuncia radicada por un importante estudio jurídico de esta Ciudad, respecto a una ex empleada por el delito de daño informático –art. 183, 2do párrafo CP-, quien, intempestivamente, dejó de concurrir a su lugar de trabajo y realizó reclamos en el fuero laboral. Tras el alejamiento de la imputada, y al buscarse diversos archivos o documentos dentro del servidor del estudio -relacionados a importantes clientes que se encontraban a cargo de la imputada-, se constató la ausencia de aquellos. Personal especializado en informática, corroboró que esos archivos fueron trabajados desde el usuario de la imputada, previo a que la misma se desvinculara del Estudio, habiendo sido borrados y copiados en un disco de almacenamiento externo. La fiscalía consideró que la denunciada habría alterado, borrado y eliminado diversos archivos de diferentes clientes del buffet en cuestión, ocasionando de esta forma un daño de difícil reparación ulterior, demandando un gran esfuerzo por parte de todos los empleados para recuperar o reconstruir los documentos, siendo que algunos de ellos no pudieron recuperarse en absoluto.

Acto seguido, se allanó su domicilio secuestrando elementos de soporte informático (CPU, notebook, pendrive, disco rígido, módem usb, etc), cuyo análisis está en pleno desarrollo.

CONCLUSIÓN

Lo expuesto en el presente informe es sólo el comienzo de un proyecto de trabajo que este equipo fiscal desarrolló a lo largo del año, con mucha responsabilidad y esfuerzo para que esta Prueba Piloto pueda convertirse en definitiva.

A lo largo de este tiempo hemos trabajado a conciencia para afrontar la complejidad en las investigaciones, el tiempo que requiere profundizarlas y la necesidad de ahondar cada uno de los puntos que hemos señalado a través de este informe, restando aún mucho por hacer.

Es de destacar el incremento incesante de casos informáticos a la justicia local, el que ha superado ampliamente las expectativas iniciales. Nótese que actualmente contamos con ciento setenta y dos **(172) casos de delitos informáticos** en trámite, sin perjuicio que, además, investigamos otros doscientos cuarenta y cuatro **(244) delitos y contravenciones comunes;** lo que eleva a un **total** de cuatrocientos dieciséis **(416) casos** los absorbidos por este equipo fiscal.

Asimismo, varios son los factores que justifican considerar que el ingreso de casos va a aumentar significativamente en un futuro inmediato:

a) Se evidencia un auge en la utilización de medios informáticos en las redes sociales y ello facilita e incrementa el uso de aquellos para delinquir

b) Cada vez es mayor la cantidad de gente que posee información acerca de cómo acceder a la justicia y denunciar inmediatamente un delito -a través de la página web del Ministerio Público Fiscal; del blog de la Fiscalía Especializada de la CABA; de Convenios con la Oficina de Protección de Datos Personales de la Defensoría del Pueblo; Convenio con el Ministerio de Justicia de la Nación; entre otros-; circunstancia que, indudablemente, provocará un aumento importante de la cantidad de ciber denuncias que ingresarán a la fiscalía especializada.

c) La conducta de ***"grooming"*** acaba de ser incorporada a nuestra legislación penal como delito autónomo. Esto, impactará en el número de denuncias a ingresar, en razón de que cada vez son más los padres preocupados en instar la acción de estas modalidades virtuales, donde son víctimas sus hijos menores de edad

d)A raíz de la experiencia piloto hemos advertido el ingreso de casos tipificados en el art. 153 bis del CP y sugerimos en consecuencia que se agregue a la resolución 501/12 la investigación del delito acceso ilegítimo a los sistemas informáticos,

Pero no solo existe una justificación o razón cuantitativa para considerar que el equipo fiscal debe continuar trabajando. Necesitamos tiempo para

desarrollar y profundizar la calidad de los objetivos fijados. Para perfeccionar los logros alcanzados; para afrontar y optimizar el desafío de la complejidad que traen aparejadas las investigaciones de delitos cometidos a través de internet y la dificultad en recolectar y preservar la evidencia digital; para aceitar los indispensables mecanismos de cooperación internacional en los casos en que la prueba se encuentra en otro país; para promover la capacitación de los operadores e investigadores que enfrentan las aristas de investigar este tipo de delitos frente al abrumador avance de la tecnología que obligan a adoptar las medidas adecuadas y eficaces para el logro de buenos resultados.

Todo ello, constituye motivo suficiente para solicitar al Sr. Fiscal General que transforme la prueba piloto del Equipo especializado en delitos informáticos, en una fiscalía que, permanentemente, pueda enfrentarse a estos desafíos, con el fin de consolidar nuestros logros y brindar a la sociedad resultados de eficiencia y eficacia en las investigaciones informáticas.

Por todo lo expuesto, solicito al Sr. Fiscal General:

1) Se transforme la Prueba Piloto del Equipo Fiscal Especializado en Delitos Informáticos en una Fiscalía que, con carácter permanente y definitivo, investigue los delitos y contravenciones informáticas y que se cometen a través de internet incluidas en la Resolución 501/12, con competencia única en toda la Ciudad Autónoma de Buenos Aires.

2) Se incluya en el grupo de delitos y contravenciones informáticas asignadas mediante Resolución 501/12, la investigación del acceso ilegítimo en un sistema informático, tipificado en el art. 153bis del C.P.

3) Se evalúe la posibilidad de incluir en idéntico sentido que en el punto precedente, la investigación de las conductas de grooming ya que fue recientemente incorporada en el Código Penal como delito autónomo

4) Se evalúe la posibilidad de disminuir la cantidad de asignaciones de delitos y contravenciones comunes pues ello dificulta el abordaje especial a la problemática con el número reducido de personal con el que hoy cuenta la fiscalía para afrontar la investigación de un total de 416 casos.

Daniela Dupuy
Fiscal a cargo del Equipo
Especializado en Delitos Informáticos

ANEXO I - JORNADAS DE CAPACITACION

JORNADAS EN QUE LA FISCALÍA ESPECIALIZADA PARTICIPÓ EN LA ORGANIZACIÓN

4tas Jornadas de Actualización del Poder Judicial de la Ciudad Autónoma de Buenos Aires –Noviembre 2012

Durante las Jornadas se desarrollaron distintos paneles sobre temas actuales que generan desafíos para los operadores del sistema. Entre ellos: la evidencia digital en el proceso penal moderno, nuevo paradigma de Salud Mental y su impacto en el fuero penal de la CABA, nuevas competencias en conductas del Régimen Penal Tributario y Mediación Penal. Uno de los paneles se centró en la evidencia digital como nuevo desafío en el proceso penal moderno, del que participaron como oradores el Dr. Marcos Salt (Abogado y profesor de la Universidad de Buenos Aires, especialista en Delitos Tecnológicos), Dr. Enrique del Carril (Cuerpo de Investigadores Judiciales), Ppal Miguel Justo (de la División Delitos Tecnológicos de la PFA) y el Ing. Gustavo Presman (perito especialista en evidencia digital).

El panel, dirigido a todos los operadores del sistema, se centró en los problemas y desafíos que entraña la investigación de los delitos informáticos o que se sirven de medios informáticos para su comisión. De esta forma se contó con la participación de peritos especialistas en el tema quienes profundizaron en la faz técnica y forense de la evidencia digital y, por otro lado, se abordaron los problemas jurídicos que acarrea esta novedosa comisión de ilícitos.

Se realizó el 14 de noviembre de 2012, en el Hotel de las Américas- Salón Libertad.

Comisión Organizadora:
Dra. María Fernanda Botana
Dra. Daniela Dupuy
Dra. María Gabriela López Iñiguez
Dra. Gabriela Marquiegui Mac Loughlin
Dra. Carolina Serjai

Delitos Informáticos y Evidencia Digital en el Proceso Penal –Abril 2013

Durante el curso se abordaron y analizaron distintos tópicos esenciales a la hora de investigar delitos informáticos o que se sirven de medios informáticos en alguna etapa del iter criminis. En esa línea, se realizó un análisis de la legislación nacional e internacional, con hincapié en la Convención de Budapest sobre Ciberdelincuencia. Asimismo, se estudiaron los distintos tipos penales como daño informático, pornografía infantil, acceso ilegítimo a sistemas informáticos y conductas aún no tipificadas como el "grooming". Por otra parte, se realizó un estudio de la afectación del derecho a la intimidad, que se evidencia a raíz de estas nuevas formas de comisión de ilícitos, como así también el tratamiento de agentes encubiertos, agente provocador, etc.

Otro de los puntos fundamentales a la hora de profundizar en estos delitos y que se desarrollaron durante el curso, fueron los problemas de Cooperación Internacional como así también su reflejo en el proceso penal. De la mano con ello, los problemas de jurisdicción, crisis del principio de territorialidad y ley aplicable como así también el acceso transfronterizo de datos y los desafíos que generan la falta de legislación y de esta forma de obligaciones específicas del sector privado para con el Estado.

Se concluyó, que todos los temas desarrollados ponían en evidencia la necesidad de una reforma procesal debido a que nuestros Códigos no receptan estas nuevas formas de comisión de ilícitos.

En una segunda parte del curso, se estudiaron los nuevos mecanismos y técnicas de investigación de delitos informáticos o cometidos por medios informáticos, a través del desarrollo de aspectos básicos de informática forense y evidencia digital. Esencialmente, se exhibieron las características técnicas y herramientas para el aseguramiento de datos, registro y secuestro de información digital, preservación de la prueba y conceptos de cadena de custodia.

Duración: 15 horas
Fechas: 8, 9, 15, 16 y 22 de abril de 2013.
Horario: de 15.00 hs a 18.00 hs.
Lugar: Sala C de audiencias del edificio Beruti 3345.
Docentes del curso:
Ingeniero Gustavo Presman
Dr. Marcos Salt
Dr. Pablo Palazzi
Ppal. Miguel Justo
Mariano Manfredi
Coordinación: Dra. Daniela Dupuy

Conferencia Regional IACA para América Latina –Mayo 2013

Se llevó a cabo la Conferencia Internacional "Administración de los Tribunales en un Mundo en Cambio", coorganizada entre el Ministerio Público Fiscal de la CABA y la International Association for Court Administration, en la Facultad de Derecho de la Universidad de Buenos Aires.

En la Conferencia, tuvieron lugar distintos paneles. Entre ellos, uno dedicado a Ciberamenazas y Cooperación Internacional, con la participación de Francisco Hernández – Fiscal especialista en Criminalidad Informática y Cooperación Internacional de Granada, España -, Carlos Chinchilla Sandi – Juez de la Sala Penal de la Corte Suprema de Costa Rica y Marcos Salt – especialista en Derecho Informático y Profesor de la Universidad de Buenos Aires, Argentina.

Se realizó del 29 al 31 de mayo de 2013, en la Universidad de Buenos Aires.

Entre los temas de interés que se han discutido durante su desarrollo, se destacó el Panel sobre Cybercrime and International Cooperation, integrado por expertos en la materia: Francisco Hernández, Fiscal especializado en Criminalidad Informática y Cooperación Internacional de Granada, España; Carlos Chinchilla Sandi, Juez de la Sala Penal de la Corte Suprema de Costa Rica; y Marcos Salt, Especialista en Derecho Informático y Profesor de la Universidad de Buenos Aires, Argentina.

Algunas de las conclusiones a las que se ha arribado, en términos generales, y el principal mensaje que se ha dejado a la extensísima audiencia que presenciaba la disertación, es que hablar de delitos informáticos sin un enfoque internacional hoy en día es imposible.

Las redes informáticas atraviesan el planeta y no se detienen ante ninguna clase de fronteras. Era solo una cuestión de tiempo para que los países más avanzados concluyeran que era indispensable modificar y modernizar sus leyes de fondo y adaptar su legislación procesal, establecer medios técnicos y procedimientos de cooperación internacional para combatir los delitos cometidos a través de Internet. Esa fue la génesis de la Convención del Ciberdelito y de otros proyectos q están actualmente en discusión en foros internacionales. Lo cierto es que la localidad del derecho debió ceder frente a la globalidad de la red; incluso en un ámbito como el derecho penal y procesal penal que siempre estuvo tan ligado a la soberanía nacional y al principio de territorialidad.

Es realmente un desafío para las Cortes y los Ministerios Públicos Fiscales trabajar en este cambio de paradigma; profundizando la capacitación y entrenamiento en la materia de todos los operadores del sistema para investigar estos delitos, y para obtener y preservar la evidencia digital; fortalecer los vínculos entre el sector público y privado, evaluar las posibilidades legales de acceso a dispositivos informáticos asociados a espacios virtuales de almacenamiento (Cloud Computing) como medidas de investigación, etc.

Jornadas de Actualización del Poder Judicial de la CABA

El día 12 de noviembre de 2013 se llevaron a cabo las Jornadas Anuales organizadas por el Centro de Formación Judicial en la Facultad de Derecho de la Universidad de Buenos Aires.

En el primer panel de las jornadas, se propuso el siguiente tema:

"INVESTIGACIÓN DE DELITOS COMETIDOS A TRAVÉS DE INTERNET"

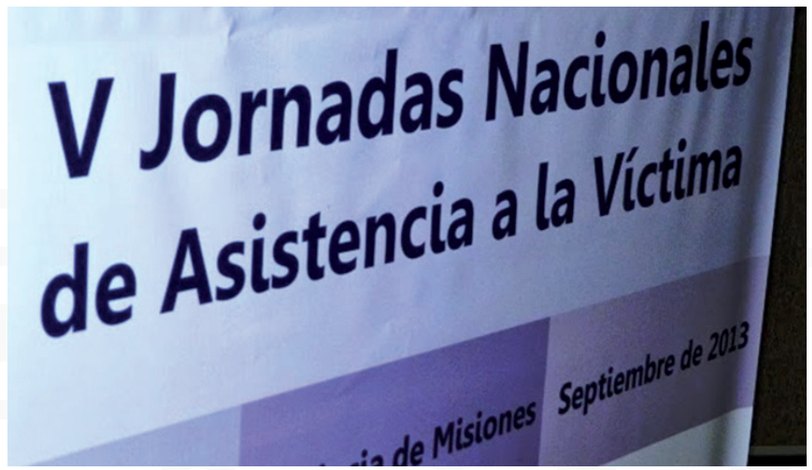
Dra. Graciela Di Letto: Determinación de la minoría de edad
Dr. Daniel Petrone: Problemas procesales durante la investigación
Dr. Marcos Salt: Problemas en la recolección de la evidencia digital
Moderadora: Dra. Daniela Dupuy

Jornadas como disertante

Taller "Por una mejor regulación de Internet en Argentina: fortaleciendo estrategias y experiencias comparadas en América Latina" –Agosto 2013

Los días 20, 21 y 22 de agosto de 2013, la Universidad de Palermo organizó el Seminario "Por una mejor regulación de Internet en Argentina: fortalecimiento, estrategias y experiencias comparadas en América Latina" – el cual fue realizado en el marco del proyecto Global Internet Freedom Program con el apoyo de Global Partners and Associates-. En el marco de dicho taller, la Dra. Daniela Dupuy expuso en el panel "Ciberdelitos, difamación y jurisdicción", donde se realizó una introducción a los ciberdelitos, se trataron aspectos de la Convención de Budapest y se discutió acerca de la necesidad o no de una nueva reforma al Código Penal luego de la sanción llamada "Ley de Delitos Informáticos"(Ley 26.038).

Jornadas Nacionales de Asistencia a la Víctima –Septiembre 2013



Los días 17 y 18 de septiembre de 2013 se llevaron a cabo las V Jornadas Nacionales de Asistencia a la Víctima, en la ciudad de Posadas, Provincia de Misiones.

Allí se analizaron los procesos de acceso a la justicia y los servicios de asistencia a las víctimas en los distintos distritos del país.

Disertaron, entre otros, el Dr. Gonzalo Sanso, titular de la Oficina de Asistencia a la Víctima de la Fiscalía General de la CABA, y la **Dra. Daniela Dupuy**, Fiscal a cargo del Equipo Especializado en Delitos Informáticos, quien expuso sobre el GROOMING como nueva modalidad delictiva cometida a través de Internet y su implicancia y actuación a las víctimas menores de edad.

Seminario de Pruebas Informáticas – Septiembre 2013

Los días 16 y 23 de septiembre de 2013, el Departamento de **Derecho de la Facultad de San Andrés organizó el Seminario sobre prueba informática**, el cual estuvo dirigido a jueces, fiscales, miembros del poder judicial, abogados, ingenieros, analistas y auditores de sistemas y programadores dependientes de empresas relacionadas con las nuevas tecnologías. Entre los temas tratados, se introdujeron aspectos básicos de la prueba informática -tanto técnicos como forenses-, la validez y el peso de la evidencia digital. También se adentró en aspectos relacionados con la cadena de custodia y los desafíos técnicos y jurídicos de la prueba electrónica.

En el marco de este Seminario, participó como disertante la Dra. Daniela Dupuy, Fiscal a cargo del Equipo Especializado en Delitos Informáticos, quien expuso acerca de la Investigación de los delitos de competencia de la CABA.

IX Seminario Internacional sobre Delitos Tecnológicos y sus Técnicas de Investigación –Octubre 2013

Entre los días 1 y 4 de octubre de 2013, se llevó a cabo el **IX Seminario Internacional sobre Delitos Tecnológicos y sus Técnicas de Investigación,** organizado por la División Delitos Tecnológicos de la Policía Federal Argentina y el cual se llevó a cabo en el Departamento Central de la Policía Federal Argentina.

El seminario se dividió en cuatro módulos: Aspectos legales del Cibercrimen, Delitos Informáticos, Delitos Financieros y Pornografía Infantil en la Web.

En el marco del primer módulo expusieron especialistas en la materia. Se contó con la presencia del Dr. Ricardo SAENZ, Fiscal de Cámara y ex presidente de la Asociación de Fiscales, quien trató principalmente los aspectos procesales Internacionales en el marco de investigaciones de delitos cometidos a través de medios informáticos, exponiendo los puntos principales del Convenio de Cibercriminalidad de Budapest y el proyecto de reforma del Código Procesal Penal de la Nación donde se estipulan cambios en cuanto a la obtención de prueba y evidencia digital, basados en el Convenio antes citado.

Luego disertó el Dr. Marcos SALT -Abogado especialista en Derecho Penal y de las Tecnologías y Profesor en Derecho Penal de la Universidad de Buenos Aires-, quien continuó con los puntos expuestos por el Dr. Saenz y trató el tema de acceso trasfronterizo de datos.

Cerraron este primer módulo la Dra. Daniela DUPUY – Fiscal especializada en Delitos Tecnológicos del Ministerio Público de la CABA- junto al Dr. Manuel DE CAMPOS -Juez Nacional en lo Criminal de Instrucción-, quienes trataron cuestiones fundamentales en la investigación.

Sus ponencias se basaron en cuatro aspectos fundamentales: la necesidad de ajuste de las leyes penales de fondo, la necesidad de reforma del CPPCABA adaptado a la obtención de prueba digital y la investigación de delitos cometidos a través de medios informáticos, la necesidad de fortalecimiento en métodos de Cooperación Internacional y, por último, la necesidad de profundizar los vínculos con el sector privado.

El Dr. De Campos finalizó su exposición tratando casos modelo en trámite ante su Juzgado haciendo hincapié en la necesidad de actualizar las técnicas de investigación en cada una de ellas.

El seminario continuó con exposiciones de expertos tanto del sector público como privado, como así también con exposiciones de personal policial de otros países, como ser de la Brigada Investigadora del Cibercrimen de la Policía de Investigaciones de Chile.

VII Jornada de Derecho y Delitos Informáticos –octubre 2013

El día 10 de octubre del corriente año se llevó a cabo la VII Jornada de Derecho y Delitos Informáticos en la Ciudad de Buenos Aires, la cual fue organizada en forma conjunta con el Programa Nacional Con Vos en la Web, Oscar Schmitz de CXO Community Latam, la Universidad del CEMA y el Centro de Protección de Datos Personales.

La jornada comenzó con un panel de "hackers vs abogados" donde se proyectaron diferentes videos y una entrevista efectuada al Director del Centro de Protección de Datos Personales, Lic. Eduardo Peduto.

Ya a la tarde, el primer panel fue el denominado "Adolescentes y jóvenes", y posteriormente en el panel denominado "Los riesgos en internet para adolescentes y jóvenes: cuando las cosas salen de la red y llegan a tribunales". Inés Tornabene –Jefa de la Oficina de Registro del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la CABA- le efectuó una entrevista a la Dra. Daniela Dupuy –titular de la Fiscalía Especializada en Delitos Informáticos-. La fiscal a lo largo de sus respuestas detalló los inicios de la Fiscalía Especializada, los diferentes delitos y contravenciones que se encuentran investigando y los distintos desafíos con los que se enfrentan día a día con su equipo de trabajo.

Lo que resaltó las Jornadas fue el panel que protagonizaron jóvenes de entre 12 y 24 años de edad, el cual fue moderado por la Lic. Lucía Fainboim, a cargo de contenidos y comunicación de "Con Vos en la Web". Los adolescentes y jóvenes opinaron sobre lo que entienden por privacidad, el distinto uso que le dan a las redes sociales y las medidas de seguridad que conocen y toman al utilizar las distintas herramientas de internet.

El último panel estuvo a cargo de Inés Tornabene, quien desarrolló varios casos reales de espionaje y se refirió a las asignaciones presupuestarias del gobierno de los Estados Unidos en diversos programas especiales de espionaje. También participó el Lic. Ezequiel Passeron – coordinador de "Con Vos en la Web"-, quien describió la gestión realizada hasta el día de hoy por el programa a su cargo.

El cierre estuvo a cargo del Lic. Eduardo Peduto, Director del Centro de Protección de Datos de la Defensoría del Pueblo de la CABA., quien trató la legislación de protección de datos personales.

ANEXO II - RESULTADO DE OPERACIÓN HISTORIA

País	Allanamientos por país	Ciudad	Arrestados o Imputados	Edad de los Arrestados	Material Incautado
Argentina	10	Buenos Aires	16	30 años	9 Desktop
		Tigre			7 Discos Duros
		González Catan			7 CD/DVD
		Banfield			3 Usb mem
		Córdoba			6 Laptop
					3 Camara
					2 Celulares
					1 SD Mem
Costa Rica	6	Heredia	3	41, 60 y 24	29 CD
		San José			7 Discos Duros
		Alajuela			19 USB MEM
					6 Desktop
					1 Laptop
					1 Ipad
España	3	Sevilla	3	----------	2 Discos Duros
		Soria		----	3 USB MEM
					200 archivos borrados de pornografía infantil

ANEXO III - RESULTADO DE OPERACIÓN HISTORIA

País	Allanamientos por país	Ciudad	Arrestados o Imputados	Edad de los Arrestados	Material Incautado
Argentina	19	Buenos Aires	30	35 años	37 Desktop
		La plata			4 Servidores
		Villa Gesell			55 Discos Duros
		Morón			2066 CD/ DVD
		Monte Chingolo			14 Usb mem
		Mar del Plata			16 Laptop
		San Miguel			19 Camara/ Video Cámara
		Córdoba			10 Celulares
		Tucumán			11 SD Mem
		Concordia Entre Ríos			3 MP3/4/5
		Reconquista			4 Routers
		San Nicolás			1 Gps
					3 Modem
					2 Grabadora de dvd
					Dinero en efectivo
Brasil	10	Nova Iguazú	4	---------- ----	---------- ---------
		Sao Paulo			
		Paraná			
		Bahía			
		Piauí			

Colombia	5	Antioquia	5	--------- ----	08 Desktop
		Bucaramanga			07 Discos Duros
		Cundinamarca			06 Laptop
					11 Usb mem
					06 SD Mem
					4 Celulares
					1 Video Cámara
					1 MP3
					850 CD/DVD
					2 Cassette DVC
					1 Cassette video 8
					1 Cassette VHS
Costa Rica	6	San José	2	45; 38.	1638 CD
		Alajuela			64 Discos Duros
		Limón			16 Usb mem
					1 Cámara
					1 Celular
					8 Desktop
					12 Laptop
					1 Ipad
Chile	13	Santiago	8	30; 35; 38; 46; 56	6 Discos Duros
		Talcahuano			2 Laptop
		Concepción			1 SD Mem
		Algarrobo			1 Usb Mem
		Rancagua			1 Servidor
		Viña del Mar			200 CD/DVD
España	21	Madrid	19	--------- ----	78 Discos Duros
		A Coruña			5 Laptop
		Granada			2 Desktop
		Orense			7 USB MEM
		Las Palmas			747 CD/DVD
		Málaga			6 Tarjetas SD
		Sevilla			1 Ebook
		Barcelona			1 Ipad
		Valencia			3 MP4
		Alicante			1 Servidor
		Zaragoza			
		Oviedo			
Ecuador	2	Quito	2	-----	-------
		Guayaquil			
Uruguay	3	Montevideo	3	23; 45; 66	3 Desktop
Venezuela	8	Caracas	5	66; 53; 42; 30	3 Discos Duros
		Miranda			4 Laptop
		Maracaibo			1 Ipad
		Portuguesa			1 USB MEM
		Aragua			1 Desktop
		Lara			1 Cámara

PROSECUTING UNIT SPECIALIZED IN CYBERCRIME

ATTORNEY GENERAL'S OFFICE OF THE AUTONOMOUS CITY OF BUENOS AIRES ARGENTINA

Team:

Daniela Dupuy

Tomás Vaccarezza

Mariana Kiefer

Catalina Neme

PRESENTATION

In November 5th, 2012, by Resolution N° 501/12, the Attorney General's Office of the Autonomous City of Buenos Aires created the Prosecuting Team Specialized in Cybercrime as a one-year pilot.

This team has a sole jurisdiction within the City of Buenos Aires and its purpose is to investigate cybercrimes as well as those crimes committed through the internet which have to be handled by specialists during the investigation process due to their complexity and hardship in identifying the implicated authors.

The team worked on a project which included the main reasons for the creation of a prosecuting unit specialized in cybercrimes. One of such reasons was the ever-increasing number of criminal behaviors related with the new technology. Another such reason was the extremely different way of carrying out these investigations as opposed to the traditional ways, since the former investigating processes require specific IT tools to detect, collect, and preserve digital evidence. Also, the creation of such a prosecuting unit was necessary because of the pressing need of implementing new working protocols related with cybercrime in order to accomplish more efficient results, among other things.

These facts, together with a series of goals set to ourselves as a specialized team, made it possible for the Attorney General of the Autonomous City of B. A. to finally entrust this challenge to us. We strongly believe that our hard work and dedication will eventually translate into another project successfully accomplished, just as we did throughout this administration.

Daniela Dupuy

Prosecutor and Head of the Prosecuting Unit Specialized in Cybercrime of the Autonomous City of B. A.

Cybercrime investigation: challenges

There are at least four key issues with which it is required to work in depth and which are also the cornerstone of this prosecuting team.

1. It is crucial to adapt substantive laws to cover the use of IT tools with criminal purposes, and to identify the web speed innovation in the national and international levels.

2. The reform of procedural laws is of vital importance. Digital evidence collection differs from physical evidence collection, to which most procedural codes of law refer.

Several topics may be discussed in order to contemplate the possibility of including them in the codes of law. Such is the case of the undercover agent; the request for preserving and obtaining data; the validity of evidence from abroad; the difference between entering physical things and entering data; the possibility of remotely applying a judicial software; jurisdiction-related issues; the use of encoding and encryption technology; etc.

Many of these topics are approached while studying the investigation scope of cybercrimes. And each of them includes different aspects which require to be expressly contemplated in substantive laws.

3. It is very important to strengthen **International Cooperation techniques.**

In many cases, data transfer procedures affect several countries. When the criminal or the party accused of a crime is not located in the same place as the victim, the investigation requires the reciprocal cooperation between the corresponding authorities of the affected countries.

4. It is crucial to forge closer bonds with **Internet Service Providers (ISP)**, since they provide vital information to us during the investigation process.

The problem is that there are no regulations whatsoever to compel ISPs to provide such information to the investigator whenever necessary.

Goals set forward and goals accomplished

- To investigate cybercrimes over which the Autonomous City of B. A. has jurisdiction, and over crimes committed through the use of computer-based means.
- To coordinate proper investigation strategies and criteria with special units from different specialized security forces, such as the Argentinean Federal Police Force and the Metropolitan Police Force, the National Military Forces, and the Body of Judicial Investigations.
- To elaborate action protocols intended to ease and unify action criteria used during the investigation process of crimes requiring digital evidence.
- To foster and promote Cooperation Agreements with the private sector for an efficient compliance with the requirements of Justice from different service providers and the different chambers gathering them.
- To jointly coordinate with the CFJ (Judicial Training Centre) the implementation of training courses on cybercrime investigation for the members of the prosecuting team, and the implementation of introductory-level action courses for all the officers of the City Department of Justice.
- To develop and exchange experiences and cooperation activities related with cybercrime between the different provinces of the country and the Autonomous City of B. A.
- To forge bonds with other organizations to coordinate applicable and useful aspects for carrying out cybercrime investigations.
- To promote the organization and implementation of training activities with countries with proven experience on cybercrime investigation.

Website of the Prosecuting Unit Specialized in Cybercrime

Thanks to the Attorney General's Office IT Department we were able to create a website of our own, which you can visit at www.delitosinformaticos.fiscalias.gob.ar. You may also visit it through the website of the Attorney General's Office of the Autonomous City of B. A.: www.fiscalias.gob.ar

Our main goals are: (1) to make known our daily work; (2) to report the news on jurisprudence and case law related to cybercrime at national and international levels; (3) to include articles by experts on cybercrime; (4) to promote training sessions on cybercrime offered by different universities and institutions.

You may report a cybercrime at our website: www.delitosinformaticos.fiscalias.gob.ar

Conclusion

The topics presented herein are just the introduction of a working project developed by this prosecuting team throughout the year with effort, dedication, and responsibility with the purpose of turning this pilot into a definite reality. But a lot of work still remains to be done.

It is worth highlighting the ever increasing number of IT-related cases entered into the local Justice –a fact that has greatly overcome the initial expectations. Please note that apart from the **172 cybercrime cases** currently in course, we have under investigation another **244 minor crimes and misdemeanors**, which brings a **total of 416 cases** being currently under investigation by this prosecuting team.

Also, there are several factors which justify the prospect of an significant increase in the number of cases to be entered in the immediate future:

a) The evident boom in the use of technological means in social networks has prompted and fueled its use with criminal purposes.

b) There is an increasing number of people who have access to Justice and know how to report a crime immediately either through the Attorney General's Office website or the blog of the Specialized Prosecuting Unit. All these facts may be also the direct result of the agreements signed with the Division of Personal Data Protection of the Ombudsman's Office or the agreement signed with the National Department of Justice, among others. Such an increasing number of people reporting crimes will undoubtedly bring a considerable rise in the number of cybercrime complaints filed in the Specialized Prosecuting Unit.

c) The act of grooming a minor online has been recently included in our criminal laws as an autonomous crime. This will have an impact over the number of cybercrime reports and complaints to be entered, since the number of parents concerned with this issue is increasing, and they are already urging the authorities to act in order to prevent such crimes and protect their children from them.

d) After the experience of the pilot we have noticed that those particular cases contemplated in section 153 bis of our Criminal Code of Law started to be entered. Accordingly, we suggest that the investigation of unlawful access to IT systems should be included in Resolution 501/12.

One single justification or quantitative reason is not enough to explain why this specialized prosecuting team has to remain operative. We need time to: (1) develop and further the quality of the goals set so as to improve what has been already accomplished; (2) face and optimize the challenge posed by the complexity inherent to cybercrime investigations and the difficulty implied in the tasks of collection and preservation of digital evidence; (3) improve the essential techniques for international cooperation in those cases in which the evidence is in another country; (4) promote the training of investigators and officers who have to face every single aspect related with the investigation process of these specific crimes while having to deal with the overwhelming progress of IT technology, all of which imposes the need to take proper measures in order to efficiently accomplish even better results.

Daniela Dupuy

Prosecutor and Head of the Prosecuting Unit Specialized in Cybercrime of the Autonomous City of B. A.

Realización - Redacción
EQUIPO ESPECIALIZADO EN DELITOS INFORMÁTICOS
Equipo de trabajo
Daniela Dupuy
Tomás Vaccarezza
Mariana Kiefer
Catalina Neme

Edición - Diseño
Carolina Saliola

Traducción
Florencia Reichart

Ministerio Público Fiscal
de la Ciudad Autónoma de Buenos Aires