

## **Reporte del Panel sobre Ciberdelincuencia y Ciberseguridad en EuroDIG 2009**

**Por: Cristos Velasco San Martín  
Director General de Ciberdelincuencia.Org**

*Cristos Velasco es un abogado especializado en regulación jurídica de internet particularmente en las áreas de privacidad, protección de datos y cibercrimen. Actualmente es el director y coordinador de Ciberdelincuencia.Org y participa y contribuye activamente en las reuniones anuales del Consejo de Europa en materia de ciberdelincuencia y en las reuniones del Foro de Gobernanza de Internet (IGF) de las Naciones Unidas.*

El pasado 14 de Septiembre de 2009 se llevó a cabo el panel titulado “*Ciberdelincuencia y Ciberseguridad: Asociaciones Público-Privadas (Cybercrime and Cyber Security Public-Private Partnerships)*”) como parte de las actividades del Diálogo Europeo sobre la Gobernanza de Internet (*European Dialogue on Internet Governance EuroDIG 2009*)<sup>1</sup> llevado a cabo en la sede del Sindicato Europeo de Transmisores (European Broadcasting Union EBU) en la ciudad de Ginebra, Suiza.

El panel fue multi-disciplinario (multi-stakeholder) y contó con la participación de Marco Gercke (Universidad de Colonia) y Hon Alun Michael (Parlamentario del Reino Unido) como moderadores; John Carr (European NGO Alliance for Child Safety Online, Reino Unido); Alexander Seger (Consejo de Europa, Francia); Michael Rotert (EuroISPA, Alemania) y; Andrea Kolb (Ministerio de Justicia de Saxony Anhalt, Alemania).

Marco Gercke abrió y dio una breve introducción acerca de la evolución histórica del cibercrimen y subrayó que una de las problemáticas actuales son los ataques a los sistemas que manejan las infraestructuras públicas, tales como las redes públicas para la explotación de servicios de telecomunicaciones, de agua, luz y gas, por medio de las cuales se proporcionan servicios básicos a la población. Señaló que tanto el cibercrimen como el número de víctimas está aumentando en distintas partes del mundo. Asimismo, destacó la importancia de castigar y penalizar los actos preparatorios para cometer delitos informáticos.

Posteriormente, Hon Alun Michael moderador del panel dio una breve presentación de los panelistas y destacó en forma muy general los temas y aspectos que se tratarían a lo largo del panel. Enfatizó sobre la necesidad de tratar temas de ciberdelito y ciberseguridad a nivel europeo y sobre todo involucrar a parlamentarios, congresistas y legisladores en ese diálogo para enriquecerlo y para crear mayor conciencia sobre la necesidad de analizar y legislar dichos temas con mayor detenimiento y puntualidad. Señaló que es de gran importancia explorar la posibilidad de llevar a cabo asociaciones público-privadas para contrarrestar el crimen informático a nivel europeo.

---

<sup>1</sup> El portal de EuroDIG 2009 se encuentra en: <http://www.eurodig.org/>

El primer panelista fue John Carr quien habló sobre la misión y las actividades de su organización. Destacó el papel que desempeña su organización en la identificación de imágenes y material sobre abuso y explotación de menores en la red y sobre la forma para prevenir su diseminación en el Reino Unido. Señaló que ese país no cuenta con estadísticas oficiales sobre pornografía de menores en la red. Hizo mención de las técnicas utilizadas para bloquear sitios por parte de la industria de ese país, a través de listas utilizadas por el Hotline y la Internet Watch Foundation (IWF) e indicó que esta última organización tiene una función quasi judicial ya que todas sus decisiones y actos se encuentran sujetos a revisión judicial. Indicó que se ha incrementado el uso de tecnologías para bloquear sitios con contenidos ofensivos, y señaló a forma de ejemplo, que están siendo utilizadas por autoridades ejecutoras y unidades sobre cibercrimen en países como EUA, México y Holanda con el propósito de reducir el tráfico y el intercambio ilícito de imágenes y contenidos. Indicó que una medida clave para poder reducir el volumen de contenidos de pornografía infantil en la red, sería mediante la localización y arresto de los individuos y redes criminales organizadas que los producen.

Posteriormente el moderador del panel Hon Alun Michael preguntó a miembros del público presente cuales otros aspectos del cibercrimen deberían ser considerados como prioritarios. Entre las respuestas, se mencionaron temas como phishing, hotlines, malware, botnets, dinero ilícito en internet, robo de identidad, ciberacoso y aspectos sobre libertad de expresión y confidencialidad de la información. Señaló que la reacción y respuesta a actividades consideradas ilícitas en el mundo real, posiblemente requieran un enfoque distinto en internet, destacando la importancia del principio de proporcionalidad en la elaboración de legislación y sobre todo el diseño de estrategias para combatir el cibercrimen por parte de la industria y de los usuarios, señalando este último punto como un enfoque preferido. En general, hubo consenso acerca de la necesidad de crear estrategias conjuntas para luchar contra el cibercrimen, las cuales deberán ser compatibles con los principios democráticos, el respeto por la dignidad y vida humana y el cumplimiento de la ley.

El segundo panelista fue Alexander Seger del Consejo de Europa (CoE) quien habló sobre un tema de gran importancia en la actualidad: “*Protección de Datos vs. Autenticación para mejorar la Seguridad*”. Seger destacó la labor del Consejo de Europa en la inclusión de los principios y aspectos tales como la protección de datos, como parte de las medidas para proteger los derechos humanos y el respeto por la ley en la UE. Señaló que la protección de datos es un elemento esencial para proteger la libertad de la información. Hizo referencia al libro ‘1984’ de George Orwell y habló sobre una resolución del Tribunal Constitucional de Alemania a principios de la década de los ochentas, en donde se declaró la inconstitucionalidad de una ley de protección de datos de ese país. Destacó que actualmente existe un gran temor y miedo de la sociedad en su conjunto sobre la creación de un nuevo “*Gran Hermano*” al momento en que las autoridades ejecutoras y los gobiernos llevan a cabo investigaciones vinculadas con conductas y actividades ilícitas en internet. También habló sobre los instrumentos existentes del CoE para la protección de los datos personales como son el *Convenio No. 108 para la Protección de los Individuos con*

respecto al Tratamiento Automatizado de Datos de Carácter Personal<sup>2</sup> el cual se encuentra abierto para firma y ratificación a cualquier país interesado en legislar en la materia.

También habló sobre los distintos retos que existen para proteger la información personal. Entre ellos, destacó el flujo transfronterizo de datos, el almacenamiento de datos como otros servicios ubicados en múltiples bases de datos y países (cloud computing)<sup>3</sup>, la interoperabilidad y el IPV6. Señaló que el anonimato representa un aspecto clave en materia de ciberseguridad, sin embargo, existe el dilema entre la adopción de medidas de seguridad por parte de las autoridades ejecutoras y gobiernos y la protección de la privacidad y la información personal del individuo como derechos fundamentales. Destacó la importancia de la adopción de lineamientos como instrumentos complementarios para combatir el cibercrimen.

Como conclusiones señaló que es necesario: (i) adoptar medidas inmediatas para contrarrestar el cibercrimen; (ii) adoptar estándares globales de privacidad y; (iii) contribuir a la democracia y al respeto por la ley.<sup>4</sup>

El tercer panelista fue Michael Rotert y habló sobre nuevas tecnologías, tendencias y amenazas. Destacó el potencial impacto de los cibercrimes en los recientes desarrollos y tendencias tecnológicas, tales como cloud computing, IPv6, DNS SEC y Web 3.0.

Hizo referencia a los lineamientos del CoE para la cooperación entre autoridades investigadoras y los ISP's en las investigaciones sobre cibercrimen<sup>5</sup>; y señaló que la industria de los ISP's se encuentra lista para cooperar con las autoridades investigadoras. Habló sobre la importancia de los Hotlines, cuya función es principalmente reportar contenidos ilícitos y enviar avisos para bajar y restringir sitios (*notice of take down*), dando como ejemplo el caso de Irlanda, en donde los Hotlines son administrados por la industria de los ISP's y han resultado sumamente eficaces.

Mencionó que las técnicas de bloqueo de sitios web resultan por un lado, excesivamente costosas, y por otro lado, pueden ser fácilmente circunvenidas y no son completamente efectivas en sistemas P2P.

También hizo mención al creciente problema de piratería de contenidos ilícitos en internet. Mencionó que con la introducción del IPV6, los cuerpos policíacos y de investigación tendrán que afrontar y verificar direcciones IP mucho más extensas, sin embargo indicó que esa tecnología proporcionará mayor seguridad al usuario final. Finalmente, subrayó que las técnicas de encriptación actuales ayudan a los delincuentes a mantener su anonimato para

---

<sup>2</sup> Convenio No. 108 del Consejo de Europa del 28 de Enero de 1981, disponible en:

[https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo\\_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-108-DEL-CONSEJO-DE-EUROPA.pdf](https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-108-DEL-CONSEJO-DE-EUROPA.pdf)

<sup>3</sup> Para mayor información acerca del Cloud Computing, ver: VELASCO SAN MARTÍN, Cristos,

“*Jurisdictional Aspects of Cloud Computing*”, 28 de Febrero de 2009, disponible en:

<http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf>

<sup>4</sup> La presentación de Alexander Seger del Consejo de Europa se encuentra en :

[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/079\\_PPT\\_cyber%20eurodig1a%20\(sep%202009\).pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/079_PPT_cyber%20eurodig1a%20(sep%202009).pdf)

<sup>5</sup> Estos Lineamientos se sometieron a discusión y se adoptaron el 2 de Abril de 2008 durante la Conferencia Anual Octopus sobre Cooperación en contra del Cibercrimen del Consejo de Europa llevada a cabo en la ciudad de Estrasburgo. Se encuentran disponibles en idioma inglés en:

[http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy\\_activity\\_Interface2008/567\\_prov-d-guidelines\\_provisional2\\_3April2008\\_en.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf)

no poder ser identificados y que el volumen de spam se ha reducido pero el phishing se ha incrementado.

La última ponente fue Andrea Kolb del Ministerio de Justicia de Saxony Anhalt en Alemania quien habló sobre la división de responsabilidades de los estados federados en ese país para combatir el cibercrimen; sobre la necesidad de garantizar la protección de los menores en línea, mediante la creación de medidas efectivas para su protección. También destacó la necesidad de conformar alianzas con redes de operadores y servicios y fomentar la cooperación internacional entre instituciones financieras y científicas, así como entre gobiernos, organizaciones no gubernamentales e instituciones privadas en contra del cibercrimen.

Posteriormente, hubo respuestas de algunos miembros del panel y se subrayó que es importante entender muy bien la problemática técnica y las soluciones jurídicas existentes. Alexander Seger hizo una puntual referencia a tres de los instrumentos más relevantes del CoE para combatir el cibercrimen y alentó a otros países a firmarlos y ratificarlos:

1. Convenio sobre la Ciberdelincuencia (*Convention on Cybercrime*)<sup>6</sup>;
2. Convenio sobre la Protección de los Menores en contra de la Explotación y el Abuso Sexual (*Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*)<sup>7</sup> y;
3. Convenio para la Protección de los Individuos con respecto al Tratamiento Automatizado de Datos de Carácter Personal (*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*).<sup>8</sup>

Finalmente, el moderador del panel Hon Alun Michael destacó a forma de conclusión tres puntos relacionados con la prevención y el marco legislativo de los delitos:

- 1. Prevenir el Cibercrimen**, mediante la identificación de individuos y organizaciones clave para evitar el abuso de menores; y la necesidad de responder con medidas efectivas y en forma más rápida;
- 2. Diseño de Estrategias** que permitan promover y proteger los derechos humanos fundamentales a la luz de las convenciones europeas y los principios existentes para su debida protección;
- 3. Una Mejor Comprensión** de la problemática sobre el cibercrimen antes de proponer soluciones para su combate; y compartir perspectivas, experiencias y mejores practicas entre todos los partícipes; y
- 4. Utilizar las Convenciones Europeas** existentes antes de crear o desarrollar otras propuestas legislativas.

---

<sup>6</sup> Convenio No. 185 del Consejo de Europa de fecha 23 de Noviembre de 2001, disponible en: [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS\\_185\\_spanish.PDF](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF)

<sup>7</sup> Convenio No. 201 del Consejo de Europa de fecha 25 de Octubre de 2007, disponible en: <http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm>

<sup>8</sup> Convenio No. 108 del Consejo de Europa del 28 de Enero de 1981, disponible en: [https://www.agpd.es/porta/web/canal/documentacion/legislacion/consejo\\_europa/convenios/common/pdfs/B.2\\_8-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf](https://www.agpd.es/porta/web/canal/documentacion/legislacion/consejo_europa/convenios/common/pdfs/B.2_8-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf)

Vale la pena señalar que los aspectos más importantes del workshop de EuroDIG 2009 servirán para preparar las contribuciones europeas correspondientes para la reunión del Foro de Gobernanza de Internet (IGF)<sup>9</sup> que se llevará a cabo del 15 al 18 de Noviembre en Sharm-El Sheik, Egipto en donde se tienen previstos algunos workshops y sesiones principales sobre cibercrimen y ciberseguridad.<sup>10</sup>

---

<sup>9</sup> El portal oficial del IGF se encuentra en: <http://www.intgovforum.org/>

<sup>10</sup> Una nota de prensa de EuroDIG 2009 se encuentra en:

<http://www.guarder.net/kleinwaechter/images/eurodig/2009/EuroDIG%20final%20press%20release%2016.09.2009.pdf>