ProtDataMx

Protección Datos México

«La protección de datos en relación a la investigación de delitos cometidos a través de sistemas de cómputo»

Dr. Cristos Velasco

Conferencia Magistral

Museo Nacional de Antropología

Xalapa, Agosto 16 de 2012

1. Introducción

Protección de la privacidad cobra cada vez mayor importancia en un mundo interconectado en donde los individuos comparten constantemente información personal con distintas entidades públicas y privadas (servicios financieros y gubernamentales, comercio electrónico, suscripciones, redes sociales, búsqueda de trabajo)

La facilidad con la que se transmiten los datos a través de Internet y el uso de tecnologías móviles permiten que las empresas y gobiernos cuentan con información detallada sobre el perfil, hábitos y ubicación de los usuarios

1. Introducción

La descentralización de servidores y la ubicuidad de los datos y la información en Internet (cloud computing, big data) son retos presentes y constantes para la protección del derecho a la privacidad de los individuos en un mundo globalizado donde Internet desconoce fronteras y límites geográficos

Cloud computing modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente (Art. 52 Reglamento LFPDPPP)

1. Introducción

"Big data, tendencia actual del sector de la TICs que permite la manipulación y control de grandes cantidades de datos personales generados por usuarios que se encuentran dispersos en distintas bases de datos y vinculados y relacionados con distintos tipos de análisis determinados para cada sector"

Las políticas publicas del big data serán analizadas por organismos internacionales tales como la OCDE y APEC.

1. Introducción

La UE tiene una población de 500 millones, muchos de los cuales tienen acceso al libre mercado laboral, de consumo y de servicios financieros. La Comisión Europea señala que 70% de los ciudadanos europeos están preocupados de que sus datos personales sean mal utilizados o destinados para fines ilícitos.

De acuerdo con el INEGI, en México reportó cerca de 38 millones de usuarios de Internet en 2011 de una población total aproximada de 113 millones de Mexicanos (Aproximadamente 33% de la población tiene acceso a Internet)

2. Protección de la Privacidad a Nivel Internacional

Diversos instrumentos internacionales contienen disposiciones sobre privacidad

- **Declaración Universal de los Derechos Humanos** (10 de Diciembre de 1948) (Artículo 12)

- **Pacto Internacional de Derechos Civiles y Políticos** (16 de Diciembre de 1996) (Artículo 17)

2. Protección de la Privacidad a Nivel Internacional

- **Convención Americana sobre Derechos Humanos** (Artículo 11)

- **Convención sobre los Derechos del Niño** (Adoptada el 20 de Noviembre de 1989, en vigor desde el 2 de Septiembre de 1990) (Artículo 16)

3. Protección de Datos en el Contexto Europeo

Cuatro instrumentos a nivel europeo que contienen disposiciones expresas sobre la protección de la vida privada y los datos personales como derechos humanos fundamentales:

(i) Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Junio 1, 2010) (Artículo 8)

(ii) Tratado sobre el Funcionamiento de la Unión Europea (Art. 16)

3. Protección de Datos en el Contexto Europeo

(iii) Carta de los Derechos Fundamentales de la Unión Europea (Arts. 7 y 8)

"Art 7. Respeto de la Vida Privada y Familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones."

"Art 8. Proteccion de Datos de Carácter Personal

1. Toda persona tiene derecho a la protección de datos de carácter personal que le conciernan.

2. Estos datos se trataran de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación."

3. Protección de Datos en el Contexto Europeo

(iv) Convenio Nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (28 de Enero de 1981)

El propósito de este convenio es garantizar, en el territorio de cada parte, a cualquier persona física independientemente de su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. (Art 1º)

3. Protección de Datos en el Contexto Europeo

El Convenio No. 108 ha sido firmado por 46 países y ratificado por 44 (27 Estados Miembros de la UE lo han ratificado)

Uruguay es el único país que ha solicitado formalmente acceso al Convenio 108 por medio del Comité Consultivo de la Convención (T-PD) en Mayo de 2011 y se espera adherirse a principios del próximo año

México ha participado como país observador en las reuniones del Comité Consultivo de la Convención (T-PD)

3. Protección de Datos en el Contexto Europeo

Secretaria General Adjunta del CoE, sostuvo una reunión con los Comisionados del IFAI en Marzo con el propósito de estrechar lazos de cooperación en materia de protección de datos y primordialmente con el fin de que México se adhiera al Protocolo del Convenio 108

30 Aniversario del Convenio 108 (Diferentes eventos y conferencias a nivel europeo, incluyendo el día internacional de la protección de datos)

3. Protección de Datos en el Contexto Europeo

Actualmente el Convenio 108 está atravesando por un proceso de modernización que comenzó el 28 de Enero de 2011 a través de una consulta pública hecha por el Secretario General del CoE precisamente para hacer frente a los retos existentes del uso de nuevas tecnologías y a recientes problemas derivados de fugas de información, acceso ilícito, etc.

Algunos objetivos que se derivaron de la consulta pública del CoE fueron:

3. Protección de Datos en el Contexto Europeo

(i) mantener la neutralidad tecnológica de las disposiciones del Convenio con disposiciones más detalladas a través de instrumentos secundarios (opiniones y recomendaciones)

(ii) mantener la coherencia y el marco jurídico de la UE en materia de protección de datos

(iii) reafirmar el potencial del Convenio 108 como un estándar internacional modelo

3. Protección de Datos en el Contexto Europeo

Durante la sesión de clausura de la Conferencia Octopus 2012, la Secretaria General Adjunta del CoE expresó : "*confirmó una vez más que las medidas contra la delincuencia informática van de la mano con la protección de los derechos humanos y el estado de derecho, que incluye la protección de los datos personales.”* Remarco que el CoE debe asegurarse de que los países adopten normas de protección de datos conforme al Convenio 108.

3. Protección de Datos en el Contexto Europeo

Protocolo Adicional al Convenio Nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal con respecto a las autoridades supervisoras y el flujo transfronterizo de datos (8 de Noviembre de 2001).

Su propósito es darle facultades de investigación y autonomía suficientes a los autoridades de protección de datos, en particular con respecto al flujo transfronterizo de datos

- Ha sido firmado por 46 países y ratificado 44 Estados.

4. Protección de Datos a Nivel Nacional

1. Constitución Política de los Estados Unidos Mexicanos

Art. 16 párrafos primero, segundo, décimo segundo y décimo tercero (Reforma Habeas Data Junio de 2009)

2. Constitución Política del Estado de Veracruz De Ignacio Llave.

"Art. 4º, tercer párrafo

Los habitantes del Estado gozaran de toda las garantías y libertades consagradas en la Constitución y en la leyes federales, los tratados internacionales, esta Constitución y las leyes que de ella emanen, así como aquellos que reconozca el Poder Judicial del Estado, sin distinción alguna de origen, raza, color, sexo, idioma, religión, opinión política, condición o actividad social."

4. Protección de Datos a Nivel Nacional

"Art. 6º. Las autoridades del Estado promoverán las condiciones necesarias para el pleno goce de la libertad, igualdad, seguridad y la no discriminación de las personas; asimismo, garantizaran el derecho al honor, a la intimidad personal y familiar y al libre desarrollo de la personalidad

Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPPP) vigente desde el 28 de Abril de 2010 (Entrada en vigor en tres distintas fases)

Reglamento de la LFPDPPP (vigente desde el 20 de Diciembre de 2011

4. Protección de Datos a Nivel Nacional

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Capítulo IV Protección de Datos Personales)

"Art. 20. Los sujetos obligados serán responsables de los datos personales, y, en relación con éstos, deberán:

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado."

4. Protección de Datos a Nivel Nacional

Decisiones y Resoluciones Judiciales

Tesis Aislada en Materia Constitucional

Tesis: 1a. CLV/2011

Agosto de 2011

Rubro: Derecho a la inviolabilidad de las comunicaciones privadas. Su objeto de protección incluye los datos que identifican la comunicación.

"El objeto de protección constitucional del **derecho a la inviolabilidad de las comunicaciones privadas**, previsto en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, no hace referencia únicamente al proceso de comunicación, sino también a aquellos **datos** que identifican la

4. Protección de Datos a Nivel Nacional

comunicación. A fin de garantizar la reserva que se predica de todo proceso comunicativo privado, resulta indispensable que los **datos** externos de la comunicación también sean protegidos.

… Estos datos, que han sido denominados habitualmente como "datos de tráfico de las comunicaciones", deberán ser objeto de análisis por parte del intérprete, a fin de determinar si su intercepción y conocimiento antijurídico resultan contrarios al derecho fundamental en cada caso concreto. Así, de modo ejemplificativo, el registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP), llevados a cabo sin las garantías necesarias para la restricción del derecho fundamental al secreto de las comunicaciones, puede provocar su vulneración.

4. Protección de Datos a Nivel Nacional

Tesis Aislada en Materia Constitucional

Tesis: 1a. CCXIV/2009

Diciembre de 2009

Rubro: Derecho a la vida privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma.

*"… En un sentido amplio, entonces, la protección constitucional de la **vida privada** implica poder conducir parte de la vida de uno protegido de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente ciertas decisiones atinentes al*

4. Protección de Datos a Nivel Nacional

propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular."

4. El Convenio sobre Cibercriminalidad del Consejo de Europa (Convenio de Budapest)

El Convenio de Budapest es un instrumento elaborado por el CoE y adoptado por el Comité de Ministros el 8 de Noviembre de 2001. Es el único tratado internacional existente para combatir el ciberdelito a nivel internacional

Tiene como objetivos: (i) armonizar los elementos sustantivos de la legislación penal relacionada con disposiciones del cibercrimen; (ii) ofrecer las facultades necesarias sobre derecho procesal para la investigación y persecución de delitos y conductas cometidas a través de sistemas de cómputo y para la obtención de pruebas en relación a la información contenida en formato electrónico

4. El Convenio de Budapest

y; (iii) establecer un régimen ágil y efectivo de cooperación internacional, entre otros objetivos

Hasta Julio de 2012, el Convenio había sido firmado por 47 Estados y ratificado por 36 países. Países no miembros del CoE que lo han firmado (Canadá, Japón, Sudáfrica y los Estados Unidos de América)

Ningún país Latinoamericano lo ha firmado, sin embargo Argentina, Colombia y la República Dominicana han aprobado y elaborado legislación y reformas a sus marcos

4. El Convenio de Budapest

jurídicos penales nacionales en materia de ciberdelitos, tomando en cuenta algunas de las disposiciones del Convenio

Invitación formal del CoE desde el año 2007 a los gobiernos de México, Costa Rica y Chile a acceder al protocolo de adhesión de la Convención (Art. 37). Ninguno de estos países ha ratificado formalmente su compromiso de acceder puesto que para ello se requiere previamente de una reforma general al marco jurídico penal tanto sustantivo como procedimental, así como la creación de CERTs y redes o puntos de contacto 24X7 nacionales para

4. El Convenio de Budapest

la identificación de conductas penales cometidas a través de internet

Durante la Conferencia Octopus 2010, hubo una sesión especialmente enfocada a analizar aspectos de seguridad y privacidad en la nube (cloud computing) en donde se discutieron definiciones, aspectos de seguridad y se hizo referencia al trabajo y la labor de otros organismos internacionales (OCDE, ENISA) con el objeto de poder establecer alianzas que ayuden a fomentar un mayor entendimiento sobre el tema y poder consensar medidas y políticas adecuadas para proteger la seguridad y la privacidad de los individuos en este entorno.

4. El Convenio de Budapest

la identificación de conductas penales cometidas a través de internet

Durante la Conferencia Octopus 2010, hubo una sesión especialmente enfocada a analizar aspectos de seguridad y privacidad en la nube (cloud computing) en donde se discutieron definiciones, aspectos de seguridad y se hizo referencia al trabajo y la labor de otros organismos internacionales (OCDE, ENISA) con el objeto de poder establecer alianzas que ayuden a fomentar un mayor entendimiento sobre el tema y poder consensar medidas y políticas adecuadas para proteger la seguridad y la privacidad de los individuos en este entorno.

4. El Convenio de Budapest

Se concluyó que el Convenio No. 108 deberá ser el estándar europeo aplicable para la protección de la privacidad y la seguridad en la nube y se recomendó su adopción por otros países para hacer frente a los aspectos regulatorios que conlleva las aplicaciones y servicios basados en la nube.

Se propuso establecer un grupo de trabajo conformado por organizaciones e instituciones privadas y públicas con el objeto de identificar mejores practicas y posibles soluciones a aspectos de seguridad y privacidad en el entorno cloud computing, así como la elaboración de

4. El Convenio de Budapest

lineamientos para los proveedores basados en la nube y las autoridades ejecutoras con relación a investigaciones transfronterizas y acceso a sistemas de datos en otras jurisdicciones

Reglamento de la LFPDPPP (Art. 52) es una de las primeras legislaciones a nivel internacional que establece obligaciones a los proveedores de cloud computing para el tratamiento de datos personales en servicios, aplicaciones e infraestructura que ofrezcan a los usuarios

5. Balance Adecuado entre Investigaciones Penales, Salvaguardias y Protección de Datos

Los gobiernos y las autoridades judiciales tienen la obligación de establecer límites y salvaguardias sobre derechos fundamentales en las investigaciones que realicen en materia de ciberdelitos.

"**Articulo 15 Condiciones y Salvaguardias**

1. Cada parte se asegurara que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente sección, se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que hayan asumido cada Parte en virtud del Convenio del Consejo de Europa para la Proteccion de los

5. Balance Adecuado entre Investigaciones Penales, Salvaguardias y Protección de Datos

los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

5. Balance Adecuado entre Investigaciones Penales, Salvaguardias y Protección de Datos

Siempre que sea conforme al interés publico, y en particular con la buena administración de la justicia, cada parte examinara los efectos de los poderes y procedimientos mencionados en la presente sección sobre los derechos, responsabilidades e intereses legítimos de terceros."

Conforme al primer párrafo, países pueden valorar libremente la forma en la que deben establecer salvaguardias y proteger derechos fundamentales tales como la protección de datos conforme a los instrumentos internacionales antes analizados.

5. Balance Adecuado entre Investigaciones Penales, Salvaguardias y Protección de Datos

Segundo párrafo establece la supervisión de ese derecho la cual puede ser a través de una autoridad judicial o alguna entidad independiente, debiendo establecer un motivo o propósito específico que justifique la investigación por parte de una autoridad, así como la duración del procedimiento

Tercero párrafo, prevé tomar en cuenta distintos intereses, entre ellos el interés público, la buena administración de la justicia y los intereses de terceras partes tales como los de ISP's que juegan un papel primordial en la investigación de ciberdelitos

5.1. Casos Europeos

La Corte Europea de Derechos Humanos (CEDH) ha emitido algunas decisiones judiciales relacionadas con la protección de la privacidad y la retención de datos en Internet como derechos fundamentales conforme a los Arts. 7º. y 8º. de la Carta de los Derechos Fundamentales de la Unión Europea

La CEDH sostiene que la protección de datos es de fundamental importancia para que un individuo pueda gozar plenamente de su derecho al respeto de la vida privada y familiar en la UE

5.1. Casos Europeos

En *Copland vs Reino Unido* de Enero de 2007 se examinó la cuestión del monitoreo de llamadas telefónicas, correo electrónico y el uso de Internet. La CEDH consideró que el almacenamiento de datos en posesión de una universidad donde el demandante había laborado implicó una injerencia en la vida privada del individuo en virtud del Artículo 8º.

En *S and Marper vs. Reino Unido* de Diciembre de 2008, la CEDH resolvió que la vida privada incluye la privacidad de las comunicaciones, la seguridad y la privacidad del correo postal, número de teléfono, correo electrónico, incluyendo la privacidad de la información.

5.1. Casos Europeos

En *Uzun vs. Alemania* de Septiembre de 2010 el Tribunal consideró que la vigilancia de un individuo a través de un sistema GPS y el uso y procesamiento de los datos obtenidos constituye una injerencia en la vida privada de la persona consagrada por el Artículo 8º.

K.U. vs Finland de Diciembre de 2008 la CEDH tomó en cuenta el Art. 8 argumentando que la invasión de la vida privada de un menor representó una amenaza a su buen desarrollo físico y mental y su vulnerabilidad a los peligros inherentes a Internet.

5.1. Casos Europeos

La CEDH estableció que si bien los usuarios de los servicios de telecomunicaciones y de Internet debe tener una garantía de confidencialidad y de libertad de expresión, dicha garantía no debería de ser absoluta y producen en ocasiones intereses legítimos tales como la prevención de desórdenes o delitos, o la protección de los derechos y libertades de terceros

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

Conferencia organizada por el CoE desde 2006 y actualmente patrocinada por Microsoft y contribuciones voluntarias de Estonia, Japón, Rumania y Reino Unido a través de una iniciativa conocida como “Proyecto sobre Cibercrimen”

Sexta Reunión llevada a cabo el 6-8 de Junio de 2012 en Estrasburgo, Francia.

Temas analizados: (1) avances en legislación sobre ciberdelitos en diferentes regiones; (2) intercambio de información entre sectores público y privado; (3) protección

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

de los menores en contra de la pornografía infantil; (4) acceso transfronterizo a datos y jurisdicción en el entorno cloud computing; y (5) estado de derecho, salvaguardias y protección de datos

280 expertos de 80 países, 15 representantes de organismos internacionales y representantes del sector privado y académico discutieron medidas para mejorar la cooperación en contra del ciberdelito y la posible revisión a algunas de las disposiciones del Convenio de Budapest

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

Participantes de México: IFAI (Comisionada Artzt apertura de la conferencia) SRE (Dirección General para temas Globales), CISEN (Dirección de Seguridad Internacional), Policía Federal (Dirección General del Laboratorio en Investigación Electrónica y Forense), la Misión Mexicana Observadora ante el Consejo de Europa, Experto en Investigación Forense y Ciberdelicuencia.Org

Mensajes Clave:

1. Estrategias para combatir el ciberdelito deben forman parte del ámbito de políticas públicas. Dichas estrategias se encuentran vinculadas a estrategias de seguridad,

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

derechos humanos, estado de derecho y la protección de datos personales. La asistencia técnica para el fortalecimiento de la capacidad en la lucha en contra el ciberdelito ayudará a las sociedades explotar el potencial de las tecnologías de la información.

2. Cooperación entre múltiples partes interesadas (multistakeholder) deberá seguir tomándose en cuenta. Esto incluye no sólo la cooperación interinstitucional, justicia penal, cooperación público- privada e internacional, sino también la cooperación entre las organizaciones internacionales, el sector académico y la sociedad civil para atender y abordar de mejor forma la problemática

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

3. Mantener el proceso de armonización global de la legislación en materia de ciberdelito conforme al Convenio de Budapest. Se reportaron avances realizados en distintos países en la adopción de legislación y aplicación del Convenio. Ejemplos: Georgia depositó el instrumento de ratificación durante la conferencia; Austria y Japón depositaron el instrumento de ratificación el pasado 13 de Junio y 3 de Julio, respectivamente. República Dominicana anunció durante la conferencia que su Congreso estaba por depositar el instrumento de firma del Convenio.

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

4. El intercambio de información público-privada, permitirá incrementar tanto la seguridad cibernética, así como la prevención y el control del ciberdelito. Los debates sugieren que es posible compartir esa información en consonancia con las normas de protección de datos. Se discutió la viabilidad de crear un grupo de trabajo para documentar buenas prácticas y ofrecer orientación.

5. El Convenio de Lanzarote y el Convenio de Budapest contienen puntos de referencia en materia de derecho penal para la protección de los menores en línea. La adopción de legislación en consonancia con estos tratados

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

permitirán un mayor ejercicio internacional de justicia penal para identificar, defender y proteger a los menores que son víctimas de explotación sexual en Internet y facilitar procesos penales a los posibles infractores. Se recomendó la organización de talleres y seminarios para apoyar la reforma legislativa en distintas regiones.

6. Los gobiernos tienen la obligación de proteger a los individuos en contra de la delincuencia y, al mismo tiempo, respetar y garantizar los derechos humanos al aplicar y ejecutar la legislación penal. Establecer condiciones y salvaguardas que limitan los poderes de ejecución por

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

parte de las autoridades ejecutoras conforme al Artículo 15 del Convenio de Budapest. Se señaló que el Convenio 108 está abierto para el acceso a cualquier país y que legislaciones en materia de protección de datos han sido adoptadas en algunos países de África, Asia y América Latina, siendo posible que algunos países puedan solicitar la adhesión formal al Convenio 108.

7. El acceso transfronterizo a datos en materia de investigaciones sobre ciberdelitos y la utilización de pruebas y evidencias electrónicas son temas de gran relevancia, en particular en el contexto del cloud computing

6. Conferencia Octopus 2012 sobre Cooperación en contra del Cibercrimen

Muchos países permiten el acceso a los datos transfronterizos, ya sea directamente o a través de proveedores de servicios bajo algunas circunstancias y condiciones. Se subrayó la necesidad de contar con normas uniformes y salvaguardias necesarias para proteger los datos personales. Los resultados del taller de trabajo se incorporarán a los trabajos del Comité de la Convención sobre Cibercrimen (TC-Y Committee) que se encuentra preparando una propuesta de un instrumento para hacer frente a este desafío. (Protocolo Adicional, Recomendación, Lineamientos, etc).

Presentación de Libro y la problemática de la Jurisdicción

7. Libertad de Expresión en Internet reconocida como Derecho Fundamental

El pasado 5 de Julio de 2012 el Consejo de Derechos Humanos de la Asamblea General de las Naciones Unidas aprobó la *Resolución A/HRC/20/L.13 Promoción, Proteccion y Disfrute de los Derechos Humanos en Internet* en la que afirma que: *"los derechos de las personas deben ser protegidos en Internet, en particular la libertad de expresión que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija"* y decide *"seguir examinando la promoción, la protección y el disfrute de los derechos humanos, incluido el derecho a la libertad de expresión en Internet y otras tecnologías, así como la forma en la que Internet puede ser un instrumento para el*

7. Libertad de Expresión en Internet reconocida como Derecho Fundamental

desarrollo y para el ejercicio de los derechos humanos de conformidad con su programa de trabajo"

La resolución tomó en cuenta el Art. 19 de la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, así como las distintas resoluciones de la Comisión de Derechos Humanos y del Consejo de Derechos Humanos de la ONU en particular la Resolución 12/16 del 2 de Octubre de 2009 y la Resolución de la Asamblea General 66/184 del 22 de Diciembre 2011

7. Libertad de Expresión en Internet reconocida como Derecho Fundamental

La resolución tuvo el apoyo de 85 países, entre ellos México y asienta un precedente importante en la protección de la libertad de expresión como un derecho fundamental en el ciberespacio.

http://tinyurl.com/93vyv7n

8. Conclusiones

Recomendamos que las autoridades encargadas de investigar y perseguir delitos, así como los tribunales judiciales en materia penal encargados de enjuiciar conductas delictivas cometidas a través de sistemas de cómputo e Internet:

I. **Respeten** los principios y garantías individuales consagradas en la Constitución Política y constituciones locales, en particular el debido proceso en materia penal, el secreto de las comunicaciones y la protección de datos personales

8. Conclusiones

II. **Tomar en cuenta** las disposiciones y principios contenidos en el Convenio 108 y el Convenio de Budapest relacionados con la protección de derechos fundamentales y salvaguardias (Art. 15) en especial la protección de la privacidad de la información de los presuntos responsables y de las víctimas en investigaciones en materia penal

III. **Implementar cabalmente** en toda investigación sobre ciberdelitos los principios internacionales de protección de datos (*fair information principles*) consagrados en tratados y lineamientos internacionales y en la legislación nacional de acceso a la información y protección de datos personales:

8. Conclusiones

Licitud. La obtención, recolección y el tratamiento de datos personales deberá hacerse con apego a la legislación nacional y el derecho internacional

Consentimiento. Referirlo y delimitarlo a un propósito o finalidad determinada en una investigación de carácter penal

Calidad. Los datos deberán ser exactos, completos, pertinentes, correctos y actualizados y cumplir la finalidad para el que fueron originalmente obtenidos y tratados

8. Conclusiones

Propósito o Finalidad. Cumplir la finalidad o el propósito lícito del destino y tratamiento de datos personales. Incluir un plazo mínimo de conservación de los datos y una vez cumplida la finalidad o propósito de una investigación, proceder a su cancelación y supresión

Lealtad. Tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, que incluyan la identidad del controlador de los datos, los sujetos obligados y el sustento jurídico para llevar a cabo su procesamiento.

8. Conclusiones

Categorías. Distinguir en forma clara el tipo de datos que pueden ser sujetos a una investigación (***Datos de tráfico o datos de contenido***) tomando en cuenta la jurisprudencia mexicana y el derecho internacional

Responsabilidad. Velar y responder por el tratamiento de los datos personales que se encuentren bajo custodia o posesión de alguna autoridad o por aquéllos que hayan sido comunicados a otra autoridad, ya sea que este última se encuentre o no en territorio mexicano. Implementar estándares y mejores prácticas internacionales

8. Conclusiones

relacionadas con salvaguardas y medidas de seguridad. Es conveniente que todas las actividades de las autoridades investigadoras sobre ciberdelitos sean debidamente registradas

IV. **Delimitar** muy bien el alcance, los límites y la competencia jurisdiccional de las autoridades encargadas de investigar y perseguir conductas relacionadas con sistemas de cómputo e Internet y el tipo y clase de datos que podrían ser sujetos de intercambio entre las propias autoridades respetando los ocho principios anteriormente señalados

8. Conclusiones

V. **Coordinarse** adecuadamente a nivel nacional e internacional para establecer medidas de cooperación que ayuden a fomentar y salvaguardar el derecho a la privacidad y la protección de datos entre organismos internacionales y regionales, autoridades investigadoras, poder judicial, autoridades de acceso a la información y protección de datos

VI. **Fomentar** una verdadera cultura de protección de la información y los datos personales en investigaciones relacionadas con ciberdelitos entre las distintas entidades

8. Conclusiones

de los sectores público, privado, académico y la sociedad civil en su conjunto. La protección de datos es y debe ser una responsabilidad compartida

VII. **Capacitar y formar** al poder judicial, las autoridades administrativas y personal encargado de la administración de justicia en la implementación de salvaguardias y la protección de los datos personales pertenecientes a presuntas partes involucradas en la comisión de delitos informáticos conforme a los tratados y convenios internacionales y mejores practicas de otros países.

8. Conclusiones

VIII. La protección de datos en el entorno electrónico y en particular en investigaciones y procedimientos relacionados con sistemas de cómputo e Internet representan **“derechos humanos de última generación”** cuya protección se debe empezar a fomentar desde las fases preliminares de la investigación y al propio interior del poder judicial federal y estatal, así como dentro de la administración de justicia en su conjunto.

Sesión de Preguntas

Preguntas

Contact information

Web: www.protecciondatos.mx

www.ciberdelincuencia.org

Email: cristosv@protecciondatos.mx