

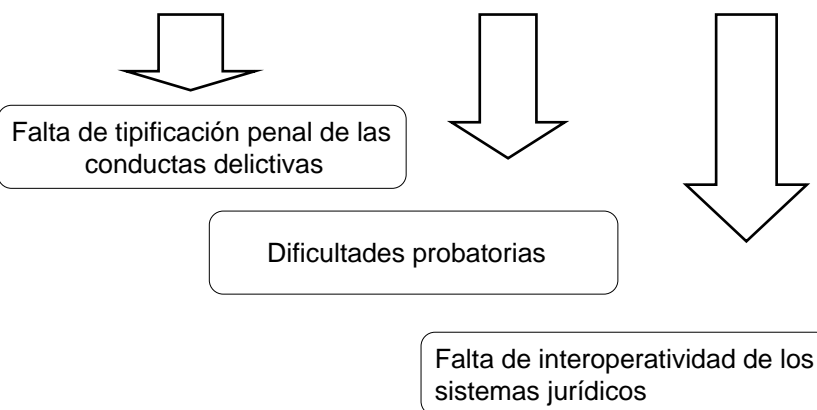
INSTITUTO UNIVERSITARIO DE LA POLICIA FEDERAL ARGENTINA

2.10.2008

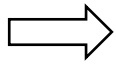
Horacio Fernández Delpech

www.hfernandezdelpech.com.ar

IMPUNIDAD DE LOS DELITOS INFORMÁTICOS

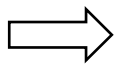


Ilícito civil



- Acto violatorio del ordenamiento jurídico que causa un daño a un tercero
- Con dolo o culpa (delito o cuasidelito)
- Indemnización por daño causado

Ilícito penal



- Tipificados expresamente por la ley penal como delito (*Principio de legalidad: El delito y la pena deben estar previstos en una ley estricta, escrita, cierta, abstracta y anterior al hecho que se juzga*)
- Se encuentra prohibida la analogía
- Con dolo o culpa (fundamentalmente dolo)
- Pena privativa de la libertad

ALGUNOS EJEMPLOS DE IMPUNIDAD POR FALTA DE TIPIFICACIÓN

El virus “Y Love You”, creado y propagado desde Filipinas por un filipino en el año 2000, creó cuantiosos daños en Europa y EE.UU.

El autor fue detenido en Manila pero debieron dejarlo de inmediato en libertad atento a que la figura del daño informático no existía como delito penal en Filipinas

EE.UU. solicitó a Filipinas la extradición del creador del virus para juzgarlo en EE.UU. en donde la conducta estaba tipificada como delito

Filipinas denegó la extradición ya que la misma no puede ser concedida por un delito que no es tal en el país al cual ha sido requerida la extradición

El 14 de Junio de 2000 se dicta en Filipinas la ley 8792 que entre otras cosas crea el delito penal de introducción de virus

En México se produjo una situación similar con el creador y distribuidor del virus W32/SirCam

Situación similar se dio en la Argentina, en varias oportunidades, Caso del hackeo de la página de la Corte Suprema de Justicia

SITUACION DE LA ARGENTINA HASTA LA SANCION DE LA LEY DE DELITOS INFORMATICOS



La falta de tipificación penal de muchas conductas delictivas producía que las mismas quedarán impunes y no pudieran ser sancionadas penalmente

"Gornstein Marcelo Hernán y otros s/delito de acción pública" Juzgado Nac.Crim.y Corr. Fed. Nº 12 Sec.24

Durante 1998 el Juzgado Criminal Nº 12 de la Capital Federal detuvo y procesó como autor del delito de daño a una persona, que en 1998 violó y dañó la página Web de la Corte Suprema de Justicia. La causa se inició en el año 1998. El acusado se encontraba en Estados Unidos, pero a su regreso el 19 de Enero de 2001, fue detenido.

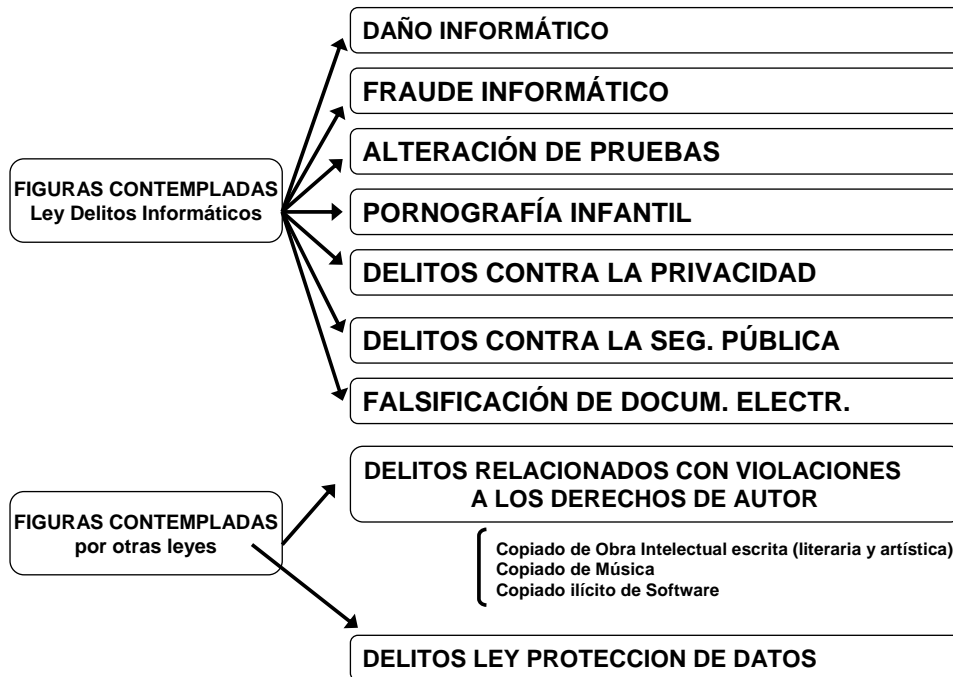
Continuada la causa se dictó fallo en el cual se absolvió al procesado por considerarse que las páginas Web no son personas, ni animales ni cosas y consecuentemente no había existido el delito de daño tipificado por el Código Penal

Idéntico criterio se aplicó en el caso **"M., Gabriel G. s/procesamiento"** En el que la Cámara Nacional Criminal y Correccional Federal, en un fallo del 2.9.2003 revocó la resolución que había decretado el procesamiento de una persona imputada, a la que se la había considerado autora responsable del delito de daño (art. 183 del Código Penal), por haber inutilizado un sistema informático

En los últimos años han existido varios Anteproyectos y Proyectos de Ley de Delitos Informáticos.

En el año 2002 incluso tuvimos un proyecto con media sanción legislativa, que finalmente no fue aprobado en la segunda Cámara

El 5.06.2008 fue sancionada la ley 26388 de Delitos Informáticos



DAÑO INFORMÁTICO

CODIGO PENAL

ARTICULO 183. - Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.

LEY DE DELITOS INFORMATICOS

Art. 10. *Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:*

“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 daños.”

“Artículo 184. La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:

15. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; 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.”

FRAUDE INFORMÁTICO

CODIGO PENAL

ARTICULO 172. - Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

ARTICULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece.....

LEY DE DELITOS INFORMATICOS

Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:

“Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.”

ALTERACIÓN DE PRUEBAS

LEY DE DELITOS INFORMATICOS

“Artículo 255. Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterar, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de SETECIENTOS CINCUENTA PESOS a DOCE MIL QUINIENTOS PESOS.”

PORNOGRAFÍA INFANTIL

LEY DE DELITOS INFORMATICOS

“Artículo 128. Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descritas 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.”

DELITOS CONTRA LA PRIVACIDAD

CODIGO PENAL

ARTICULO 153. - Será reprimido con prisión de quince días a seis meses, el que abriere indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia que no le esté dirigida.

Se le aplicará prisión de un mes a un año, si el culpable comunicare a otro o publicare el contenido de la carta, escrito o despacho.

LEY DE DELITOS INFORMATICOS

“Artículo 153. *Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.*

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.”

“Artículo 153 bis. *Será reprimido con prisión de quince días a seis 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 mes a un 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.”

“Artículo 155. *Será reprimido con multa de pesos UN MIL QUINIENTOS (\$1.500) a PESOS CIEN MIL (\$100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.*

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.”

“Artículo 157. Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.”

“Artículo 157 Bis. Será reprimido con la pena de prisión de un mes a dos años el que:

- 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;***
- 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.***
- 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.***

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.”

DELITOS CONTRA LA SEGURIDAD PÚBLICA INTERRUPCIÓN DE LAS COMUNICACIONES

LEY DE DELITOS INFORMATICOS

“Artículo 197. Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida

FALSIFICACIÓN DE DOCUMENTOS ELECTRÓNICOS O INFORMÁTICOS

LEY DE DELITOS INFORMATICOS

Art. 77 del Código Penal

"El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, Almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente."

II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

DELITOS RELACIONADOS CON VIOLACIONES A LOS DERECHOS DE AUTOR

Fundamentalmente reproducción sin la
autorización del titular de los derechos

Obra Intelectual (artística, dram.)

Conforme la ley 11723

- Ilícito civil
- Ilícito penal (aunque sea para uso privado y sin fines de lucro)

En EE.UU. la reproducción para uso privado no es delito penal (fair use), en España tampoco

Obra Musical (fonograma)

Conforme la ley 11723
con modif.ley 23741/89

- Ilícito civil
- Ilícito penal (solo cuando sea con fines de lucro)

Software

Conforme la ley 11723
con modif.ley 25036/98

- Ilícito civil
- Ilícito penal (aunque sea para uso privado y sin fines de lucro)

Fallo del año 2000 condeno a tres meses de prisión en Suspenseo y multade \$ 500

II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

DELITOS CREADOS POR LA LEY DE PROTECCION DE DATOS E INCORPORADOS AL CODIGO PENAL

Artículo 117 bis del Código Penal:

- 1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
- 2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales
- 3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
- 4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

Artículo 157 bis del Código Penal:

"Será reprimido con la pena de prisión de un mes a dos años el que:

- 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
 - 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.
- Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

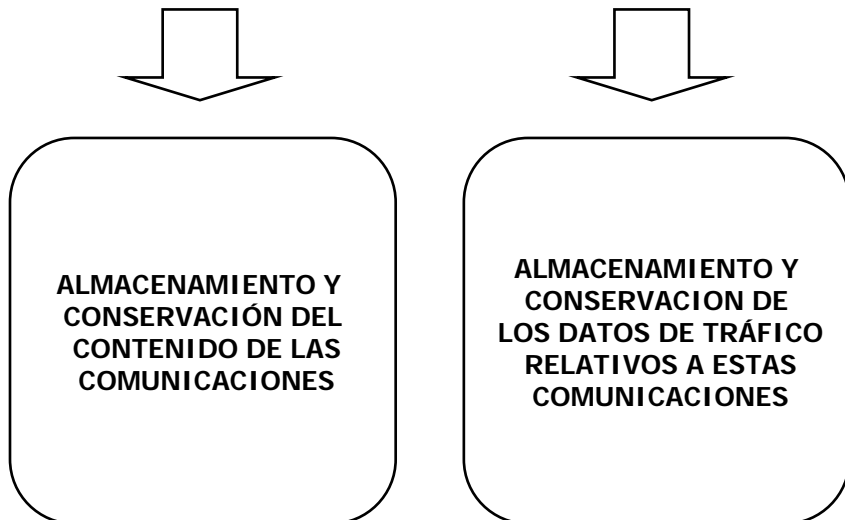
II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

La conservación de datos de trafico es una importante forma de colaboración en la investigación de la delincuencia informática

No se debe confundir con la conservación de los contenidos

II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

**Conservación de datos por parte de los ISP
Dos situaciones diferentes:**



II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

**ALMACENAMIENTO Y CONSERVACIÓN DEL CONTENIDO
DE LAS COMUNICACIONES**

El **deber de confidencialidad** es una de las principales obligaciones del transportador de un correo electrónico, quien:

- No puede revelar a terceros el contenido de los correos transmitidos;
- Debe adoptar las medidas técnicas y de seguridad necesarias para que esa confidencialidad no pueda ser violada por terceros;

EL CONTENIDO QUE SE HA TRANSMITIDO NO DEBE SER CONSERVADO POR EL ISP, salvo:

- El almacenamiento automático, transitorio y necesario para llevar a cabo la transmisión;
- Cuando la ley expresamente así lo establezca y por el tiempo y modalidades establecidas en la misma;
- Cuando las partes intervinientes en la transmisión, así lo hayan solicitado;

FUERA DE ESTOS SUPUESTOS NO DEBE SER ADMITIDO EL ALMACENAMIENTO YA QUE VIOLA EL DERECHO A LA PRIVACIDAD

ALMACENAMIENTO Y CONSERVACION DE LOS DATOS DE TRÁFICO RELATIVOS A LAS COMUNICACIONES

En Doctrina y Legislación Internacional es hoy motivo de debate si los ISP deben conservar los datos de tráfico durante algún lapso de tiempo.

Se discute también que debe entenderse por datos de tráfico. En general se entiende, que se refiere a todos los elementos que hacen a la individualización de partida y llegada, fecha, hora y demás datos, que no impliquen la vulneración y conocimiento del texto contenido en el mensaje.

ARGUMENTOS A FAVOR DE LA CONSERVACION

- Seguridad Nacional
- Investigación de delitos;
- Dar cabida a la prueba del correo electrónico en los regímenes procesales;

ARGUMENTOS EN CONTRA DE LA CONSERVACION

- Afectación de la Intimidad y Privacidad
- Altísimo costo que esta obligación genera para los ISP

II Jornadas de Derecho Informático – Instituto Universitario Policía Federal
Horacio Fernández Delpech

ALMACENAMIENTO Y CONSERVACION DE LOS DATOS DE TRÁFICO EN LA UNIÓN EUROPEA

Directiva General 95/46/CE } Aceptaban el almacenamiento de los
Directiva 97/66/CE } datos de tráfico al solo efecto de la
facturación

La **Directiva 2002/58/CE** (*Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Comunicaciones*), faculta a los estados a establecer excepciones a las normas de destrucción de datos de tráfico, para proteger la seguridad y la defensa nacional.

En el art.15 se autoriza a los estados a retener datos de tráfico para prevenir e investigar delitos.

A partir de entonces los estados europeos están estudiando el dictado de normativas relativas a la retención de los datos de tráfico mas allá de la finalidad de la facturación.

DECISIÓN MARCO SOBRE RETENCIÓN DE DATOS DE TRÁFICO DE DE COMUNICACIONES ELECTRÓNICAS

El 28 de abril de 2004 el Reino Unido, Francia, Irlanda y Suecia, han Presentado esta propuesta que pretende armonizar en los Estados Europeos normas mínimas sobre la retención de datos de tráfico, dada la importancia que se considera que dichos datos tienen hoy en día en la investigación de delitos graves, incluido el terrorismo.

NUEVA DIRECTIVA EUROPEA (Directiva 2006/24/CE)

El 21.02.06 el Consejo de Ministros de la Unión Europea aprobó la Directiva sobre retención de datos de tráfico telefónicos y de comunicaciones electrónicas que obliga a los operadores de telecomunicaciones a almacenar los datos durante un período de entre 6 y 24 meses.

Principales características:

- Finalidad: fines de investigación, detección y enjuiciamiento de delitos graves tal como se definen en la legislación nacional de cada estado
- Los datos a retener serán «los necesarios para localizar e identificar la fuente de una comunicación
- No se aplicará al contenido de las comunicaciones
- En el art 5 se detallan cuales son los datos de tráfico y de localización y datos relacionados que deben retenerse
- La Directiva establece un plazo de 18 meses para que los Estados miembros de la UE incorporen la norma a sus legislaciones internas.

AUSTRIA - Se esta estudiando incluirlo en el proyecto de ley de comunicaciones

BELGICA - La Computer Crime Act (28 Nov. 2000) admite para investigación criminal pero no se encuentra aun reglamentado

DINAMARCA - La Sec.786 de la ley de Administración de Justicia, admite para invest. policial por un año, pero no se encuentra aun vigente pues debe ser reglamentada

FINLANDIA - Apoya su implementación por un periodo de dos años, pero aun no ha sido establecida

FRANCIA - Se admite a los efectos de la investigación criminal por un año

ALEMANIA - no se admite

IRLANDA - Se admite por tres años

GRECIA - Existe una tendencia a aceptarlo por un año

GRAN BRETAÑA - The Anti-Terrorism Crime and Security Act was passed in 2001, Part 11, lo permite a los fines de la seguridad nacional o la lucha contra el delito

SUECIA - Es un tema actual de discusión, se sugiere 12 meses como mínimo


Austria - No se admite

España - Art. 12 de la LSSICE

EE. UU. - Acta Patriotica

ALMACENAMIENTO Y CONSERVACIÓN DE LOS DATOS EN ARGENTINA

La **Ley 25873** dictada el 17.12.2003 modificó la **Ley 19758 de Telecomunicaciones**, incorporando nuevos artículos al texto estableciendo:

- Autoriza la interceptación de las comunicaciones telefónicas o por Internet, incluido los contenidos, pero supeditando esta interceptación a la previa orden judicial o del Min. Publico. Reafirmó así lo que dispone la ley 25520 de Inteligencia Nacional. 
- Establece la obligación de conservación de los datos de tráfico de las comunicaciones por parte de las empresas prestadoras de los servicios y por el término de diez años, con la finalidad de su consulta por parte del Poder Judicial.

El **Decreto 1563**, de Noviembre de 2004, reglamentó la ley 25873

A resultados de la polémica desatada

- Se dictó el **Decreto 357/2005** que suspendió la aplicación del Decreto 1563
- La Justicia estableció su inconstitucionalidad. (**Recurso amparo CABASE**)
- La Justicia estableció su inconstitucionalidad. (**Halabi vs.Estado Nac.**)

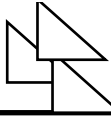
Ley 25520 de Inteligencia Nacional

Art.18:cuando en el desarrollo de la actividad de inteligencia o contrainteligencia sea necesario realizar interceptaciones o captaciones de comunicaciones privadas de cualquier tipo, la Secretaria de Inteligencia deberá solicitar la pertinente autorización judicial...

Convenio sobre Cibercriminalidad

ETS 185– Budapest 23.11.2001

- Fue elaborado por el Consejo de Europa conjuntamente con EE.UU., Canadá, Japón y Sud Africa y abierto para las firmas en Noviembre de 2001, a la fecha firmado por 43 estados;
- Tiene un protocolo adicional del 2003 contra el racismo y la xenofobia;
- Pretende homogenizar las leyes penales sobre criminalidad en el ciberespacio para proteger los derechos de los ciudadanos y perseguir la delincuencia entre países;
- Dispone la creación como figuras penales de una serie de conductas, estableciendo: *“Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal..”*
- Dispone también la adopción de medidas procesales, de conservación de datos de trafico, sobre extradición, colaboración entre estados, etc.
- La reciente ley de delitos informáticos menciona haber tenido en cuenta las previsiones del Convenio



Muchas gracias

www.hfernandezdelpech.com.ar

hfernandez@hfernandezdelpech.com.ar