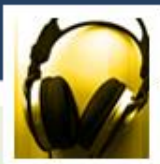
El cibercrimen como fenómeno criminológico

Abordaje y políticas para el sector

Internet


- ✓ Red de computadoras creada por el Departamento de Defensa de los Estados Unidos a fines de la década del 60 en el marco de la Guerra Fría.
- ✓ Objetivo: crear un medio de comunicación **flexible** y **descentralizado** frente a un posible ataque nuclear soviético.

Internet

Flexible:

- ✓ La información que se transmite por Internet se fracciona diferentes **paquetes de datos** que viajan por vías de comunicación alternativas hacia la dirección de destino asignada.
- ✓ Funciona en base a **ensayo y error**. Si un punto de la red la comunicación falla, ese paquete vuelve al punto de origen junto con el resto para ser reenviado nuevamente.

Internet

Descentralizada:

- ✓ No posee un centro por donde pasan todos los contenidos.
- ✓ En realidad es una **red de redes** de dispositivos independientes -cada una con su estructura y configuración propia- que se interconectan entre sí por el uso común de un protocolo de comunicaciones.

Internet

- ✓ Internet no salía de las fronteras de los Estados Unidos.
- ✓ No había necesidad de regulación en términos de seguridad de las comunicaciones en tanto interconectaba centros de investigación universitarios, laboratorios de empresas contratistas del ejercito y organismos gubernamentales.

Internet

Factor estructural en términos criminológicos:

- ✓ El diseño de Internet no fue pensado en términos de la seguridad de las comunicaciones -los datos y la información que se transmiten- sino en la seguridad física de las redes.
- ✓ En la actualidad -aunque mejorados- los protocolos de comunicación son los mismos.

Historia de los delitos informáticos

- ✓ Durante la década del 60 e influenciada con la obra “1984” de Orwell comienza a cuestionarse el uso de la informática en términos de privacidad e intimidad de las personas.
- ✓ Con la recolección, el almacenamiento y transmisión de datos e información a través dispositivos informáticos aparecen las primeras conductas indebidas y hechos ilícitos relacionados con computadoras.

Historia de los delitos informáticos

Década del 70: Primeros casos registrados de delitos informáticos, en su mayoría, sabotajes a bases de datos digitalizadas con **fines económicos y comerciales:**

- ✓ Alteración de saldos y balances de empresas para el pago de facturas y salarios (fraude)
- ✓ Robo de las agendas de contactos de clientes de las grandes corporaciones (espionaje comercial).
- ✓ Con la digitalización de obras protegidas por el derecho de autor comienza a tener lugar la “piratería” de software (violación a la leyes de prop. Intelectual)

Historia de los delitos informáticos

Década del 80:

- ✓ Casos de fraudes en cajeros automáticos a tarjetas de debito a partir de dispositivos lectores de las bandas magnéticas (Falsificación)
- ✓ Contenidos ilícitos y nocivos en las redes (amenazas, discriminación, distribución de pornografia infantil)
- ✓ Ataques contra la vida: manipulación de sistemas de vuelo y bases de datos hospitalarias o de salud (hacking).

Criminología del cibercrimen

- ✓ Algunos estudios identificaban a los delitos informáticos como **delitos de cuello blanco,** termino acuñada por el sociólogo estadounidense Edwin Sutherland en 1939.
- ✓ Refiere a los delitos cometidos por los hombres de negocios a partir de la posición de poder que ocupan desde las corporaciones.

Criminología del cibercrimen

Definición:

- ✓ El delito de cuello blanco es cometido por personas de respetabilidad y status social alto en el curso de su ocupación (empresarios). Asimismo tiene la capacidad de generar temor y admiración en la gente por producir ingresos en forma ilícita sin ser alcanzados por la justicia.

Criminologia del cibercrimen

- ✓ Hasta principios de los años 80s, los usuarios de informática debían tener conocimientos específicos para el manejo de computadoras. El funcionamiento de los dispositivos estaba basado en programas que operaban mediante comandos complejos que requerían de formación y capacitación específica.

Criminología del cibercrimen

- ✓ Los hackers **no eran gente de negocios** y la mayoría de las veces se revelaban contra ellos a partir de un espíritu cuasi anárquico y libertario.
- ✓ Muchos de ellos bregan por **la libertad de expresión y el derecho a la información en Internet** y se manifiestaban contra los gobiernos y las empresas que ellos consideran afectan estos principios.

Criminología del cibercrimen

Gary Green, criminólogo estadounidense (1990)

Concepto de delito ocupacional:

"Cualquier acto penado por la ley que se comete a partir de las oportunidades generadas en el transcurso de una ocupación que es legal"

Criminología del cibercrimen

Categorías de **delitos ocupacionales**:

- ✓ Delitos **organizacionales**
- ✓ Delitos **gubernamentales**
- ✓ Delitos **profesionales**
- ✓ Delitos **cometidos por personas que son parte de una organización** en su propio beneficio.

Criminología del cibercrimen

El cibercrimen surge como un tipo de **delito ocupacional de tipo profesional:**

- ✓ Los primeros usuarios de Internet eran en su mayoría ingenieros, programadores y especialistas en informática que requería de secretismo de sus actividades.
- ✓ Actos cometidos en el ejercicio de su ocupación a partir de las posibilidades que le brindaba su medio laboral, a saber, el acceso a computadora y redes.

Surgimiento de la Internet Comercial

- ✓ Principios de los 80s: creación de la **computadora personal** (PC
- ✓ Desarrollo de primeros programas y aplicaciones de uso domestico y entornos gráficos que van sustituyendo a los comandos escritos en lenguajes de programación específicos.
- ✓ En 1990 se crea la **World Wide Web**, el servicio mas popular de Internet junto al correo electrónico.

Surgimiento de la Internet Comercial

- ✓ Ya finalizada la Guerra fría, en 1995 la Administración norteamericana abre públicamente Internet al resto del mundo para el desarrollo de *“la infraestructura global de la Información”.*

- ✓ Con el desarrollo de la **Internet Comercial**, los bancos y las empresas comienzan a desembarcar en la red para ofrecer productos y servicios en linea.

Surgimiento de la Internet Comercial

EEUU: apertura publica y expansión global de la red

- ✓ Fin: Desarrollo de una economía digital para el desarrollo de la modalidad de negocios del Siglo XXI:

El comercio electrónico

Delitos informáticos

Con la expansión global y el uso cotidiano de Internet, adquiere una nueva dimensión concepto de **delitos informáticos.**

Delitos informáticos

Criterios de conceptualización:

- ✓ **Criterio técnico:** computadoras, dispositivos automatizados en general, dispositivos electrónicos, tecnologías de la información, entre otros.
- ✓ **Criterio legal:** hechos ilegales, actos ilícitos, conductas indebidas o no éticas, conductas no autorizadas, etc.

Delitos informáticos

- ✓ **El entorno como criterio de clasificación**:

Majid Yar:

“La delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino mas bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar”.

Delitos informáticos

- ✓ **Criterio criminalístico:**

Solo son considerados delitos de tipo informáticos solo aquellos que requieren de una **pericia informática** para la resolución de un caso.

Delitos informáticos

- ✓No refieren a un tipo de criminalidad específica.
- ✓Adquieren esta definición a partir del **lugar que ocupa la tecnología** mas que a la naturaleza criminal del acto mismo.

Delitos informáticos

Definición más generalizada en la actualidad:

- ✓ Conductas indebidas e ilícitas que utilizan un dispositivo informático como ***medio*** para la comisión de un delito o como ***fin*** del delito mismo.

Delitos informáticos

En la actualidad el cibercrimen se explica a partir del **criterio de oportunidad:**

- ✓ A partir las posibilidades que brinda un medio global, de fácil acceso y con la posibilidad de acceder a miles de personas a partir del uso de servicios y aplicaciones de Internet en forma gratuita.

Delitos informaticos

Clasificación de delitos informáticos que se cometen por Internet:

- ❖ Aquellas conductas ilícitas que se cometen a través de programas maliciosos (virus, gusanos, troyanos, spyware, ransomware) y tienden a afectar la integridad de los dispositivos o la confidencialidad y seguridad de los datos e información:

- ✓ Requieren de una **ingeniería técnica** para su comisión

Delitos informáticos

Clasificación de delitos informáticosque se cometen por Internet:

- ❖ Aquellos delitos convencionales que no necesitan de un programa para su comisión y utilizan servicios y aplicaciones de Internet como medio para su comisión técnicas de **ingeniería social**
- ✓ Suplantacion de identidad, fraudes, estafas, agresiones, amenazas, acoso (grooming, ciberbullying), etc.

Delitos informáticos

Clasificación de delitos informáticos que se cometen por Internet:

- ❖ Todos aquellos que se vinculan a la privacidad de las comunicaciones personales y el derecho a la intimidad de los usuarios

- ✓ **Intervenciones ilícitas por parte de los gobiernos en materia de seguridad**
- ✓ **Violación a la intimidad de los ISPs en términos comerciales**
- ✓ **Uso de la informática en el ámbito laboral**

Delitos informáticos

Áreas de abordaje del cibercrimen como fenómeno criminológico:

- **Derecho**
- **Seguridad informática**

Delitos informáticos

Derecho: aborda la problemática a partir de la tipificación de conductas ilícitas relacionadas con dispositivos informáticos y las diferentes alternativas para la persecución penal de este tipo de conductas.

- ✓ Es una *perspectiva sancionatoria* basada en la conjuración y represión del delito.

Delitos informáticos

- ✓ **La seguridad informática:** aborda la problemática desde el punto de vista técnico a través de medidas de protección de los dispositivos (software y hardware) para el resguardo de la confidencialidad, integridad y disponibilidad de los datos e información.
- ✓ Es una *perspectiva técnico preventiva*.

Derecho y nuevas tecnologías

Primeras **medidas de tipo legales** en la Internet comercial en materia de seguridad:

- ✓ Protección legal de los datos y la información digital y los dispositivos informáticos como bienes jurídicos.
- ✓ Reconocimiento legal de las empresas que operan en la red.
- ✓ Regulación de actividades de compraventa de productos y ofrecimiento de servicios online.
- ✓ Sanciones comerciales, civiles, administrativas y penales frente a conductas indebidas, antiéticas e ilícitas que se presentan en la red.

Seguridad informática e internet

Primeras **medidas de tipo técnicas** en la Internet comercial en materia de seguridad en la red:

- ❖ Desarrollo y aplicación de sistemas de encriptación de comunicaciones en línea para la transmisión de datos e información financiera de los usuarios para el uso de sistemas de pago de pago electrónicos:

- ✓ Homebanking, sitios de subastas y tiendas en línea, casinos en línea, sitios web pornográficos.

Derecho y nuevas tecnologías

Estrategia en materia de cibercrimen:

A nivel país:

- ✓ Tipificación de conductas relacionadas con dispositivos informáticos y reconocimiento legal de los datos e información digital.
- ✓ Establecimiento de herramientas legales para la investigación de delitos informáticos.

Derecho y nuevas tecnologías

A nivel internacional:

- ✓ **Armonización penal** de conductas relacionadas con delitos informáticos
- ✓ Fortalecimiento de la cooperación internacional en materia de investigación criminal

Derecho y nuevas tecnologías

- ✓ En 2001, en el marco del Comité de Ministros del Consejo de Europa se firma el "**Convenio sobre Cibercriminalidad de Budapest"** con el objetivo de armonizar las legislaciones penales de los 47 estados miembros en materia de delitos informáticos.
- ✓ En la actualidad es el documento de referencia más importante a nivel mundial en materia de **Derecho Penal, Procesal Penal y cooperación internacional.**

Derecho y nuevas tecnologías

Legislación penal en Argentina:

- ✓ Aplicación de tipos penales convencionales para la protección de la información digital.
- ✓ Modificación de normativas para actualizar antiguas figuras en términos de delitos informáticos.
- ✓ Promulgación de leyes especificas en el área.

Derecho y nuevas tecnologías

Argentina (1996):

- ✓ **Modificación de la ley 24.766 de secretos comerciales**:

  Tipifica la sustracción de secretos comerciales contenidos en soportes electrónicos

- ✓ **Actualización del Régimen Penal Tributario:**

  Pena la sustracción adulteración o falsificación de documentos electrónicos en la Administración Pública Nacional

Derecho y nuevas tecnologías

- 1998: Modificación de la **Ley Nº 11.723 de Propiedad Intelectual** pena la copia ilegítima de cualquier programa de software o base de datos informática.
- 2000: Primeras leyes relacionadas con la confidencialidad de los datos con la **Ley Nº 25.326 de Protección de Datos Personales**; y con la integridad y autenticidad de la información con la **Ley Nº 25.506 de Firma Digital.**

Derecho y nuevas tecnologías

2008:

- Ley Nº 26.388 o **“Ley de delitos informáticos”:**

- ✓ Establece 10 figuras penales relacionadas con la protección de delitos relacionados con dispositivos informáticos

Derecho y nuevas tecnologías

2010: Argentina manifiesta la adhesión al Convenio de Budapest en la reunión quinquenal del Consejo de Europa en Estrasburgo (Francia).

2011: Proyecto de reforma del código procesal penal.

Proyecto no fue presentado en el parlamento para su ratificación en tanto tratado internacional.

Derecho y nuevas tecnologías

2017:

- ✓ Presentación de proyecto para la aprobación en el Senado Nacional
- ✓ Abril: obtiene media sanción en la Cámara Alta.
- ✓ Actualmente se encuentra en tratamiento en las comisiones de Relaciones Exteriores y Legislación Penal de la Cámara de Diputados

Seguridad Informática

1999:

- Se crea en el ámbito de la APN la Coordinación de Emergencias en Redes Teleinformáticas (ArCert) mediante resolución de la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros de la Nación.

Seguridad informática

Funciones:

- ✓ Prevención, detección y manejo de incidentes de seguridad en redes informáticas de los organismos la APN.
- ✓ Recomendar herramientas y técnicas para elevar los niveles de seguridad de los sistemas.

Seguridad informática

Funciones:

- ✓ Asesoramiento técnico de seguridad a nivel organizacional para el manejo de incidentes.
- ✓ Elaborar reportes de amenazas y ataques a los fines preventivos o correctivos.

Seguridad informática

- Constaba de un **Comité Asesor**, integrado por un grupo de especialistas que conforman el *equipo de seguridad en redes* profesionales en la materia dedicados a investigar sobre incidentes y brindar recomendaciones ante consultas específicas

Seguridad informática

Miembros asociados:

- ✓ **Usuarios plenos:** organismos de la Administración Publica Nacional
- ✓ **Usuarios simples:** organismos de las administraciones públicas provinciales y/o municipales y organizaciones relacionadas con la SI.
- ✓ **Publico en general**

Seguridad informatica

2011:

- ✓ Se crea el **Programa Nacional de Infraestructuras Críticas de la Información (ICIC)** en el seno de la Dirección Nacional de Infraestructuras Críticas de la Jefatura de Gabinete de Ministros de la Nación.

Seguridad informática

Modelo de referencia:

- **CERT** en los EEUU y **CSIRTs** en Europa:

- ✓ El primer CERT fue creado en 1988 en el seno de DARPA a partir de la infección del 10% de las computadoras conectadas a la red ARPANET por el Gusano Morris

Seguridad informática

CERTs

- **Política de no revelación de vulnerabilidades informáticas de los sistemas de los proveedores**:

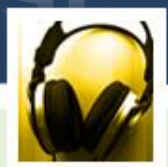
- ✓ Hasta el año 2001 una vez solucionadas eran las mismas organizaciones quienes las informaban.
- ✓ A partir de ese una vez notificado de la misma por parte del CERT tiene 45 días para publicarla.

Investigación criminal

Dificultades en términos de investigación criminal:

- ✓ Con el surgimiento de la Web, fue necesario crear un organismo global que coordine la asignación de direcciones para que los usuarios accedan a los sitios.
- ✓ En 1998 se crea la Corporación para la Asignación de Nombres y Números de Internet (ICANN) con sede en Estados Unidos.

Investigación criminal


Primera dificultad en términos de investigación criminal:

- ✓ La función principal de éstos organismos no es verificar quienes son sus titulares ni cual es la finalidad del sitio web, sino que las direcciones **no se repitan.**
- ✓ Estas entidades desarrollan una **función puramente técnica.**

Investigación criminal

Identificación de usuarios:

- ✓ Internet permite la **construcción de identidades ficticias**: La mayoría de los servicios y aplicaciones web son gratuitos y solicitan a las personas nombre de usuario y contraseña y/o una dirección de correo.

Investigación criminal

Identificación de usuarios:

- ✓ Existe a posibilidad de **no conocer la identidad real** de una persona detrás de la pantalla: En caso de comunicaciones escritas no existen rasgos personales del usuario (estilo de escritura, voz, fotografía)

Investigación criminal

Identificación de usuarios:

- ✓ Solo se puede conocer **la ubicación del dispositivo** desde donde estableció la comunicación.
- ✓ Dirección IP: cada dispositivo conectado a Internet posee una identificación numérica única de cuatro dígitos.

Investigación criminal

Segunda dificultad en términos de investigación criminal**:**

- ✓ **Las comunicaciones en Internet pueden ser completamente anónimas.**
- ✓ En el marco de una investigación criminal, la persecución penal del autor de un delito puede verse frustrada por la falta de elementos probatorios.

Investigación criminal

Tercera dificultad en términos de investigación criminal:

- ✓ **La ausencia de un ente centralizado donde realizar requisitorias de información**.

Gobierno de Internet: Asociaciones sin fines de lucro de carácter global que establecen cambios técnicos para la red (ICANN, ISOC, W3C)

Investigacion criminal

Cuarta dificultad en términos de investigación criminal:

Territorialidad, jurisdicción y competencia judicial:

- ✓ El delito informático cometido en al nube es transnacional per se
- ✓ Escena del crimen: no espacio físico sino entorno digital

Investigación criminal

Requisitorias de información a empresas proveedoras de servicios de Internet en términos de información de usuarios y comunicaciones privadas (con orden judicial)

- ✓ **La empresa no tiene representación legal en el país**, por el cual la solicitud se debe cursar mediante exhorto al país donde figure su sede legal.

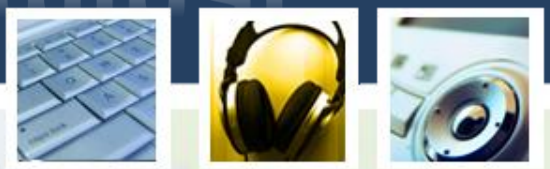
Investigación criminal

- ✓ El proveedor de servicios tiene representación legal en el país, pero **los servidores se encuentran en el extranjero** y debe realizar la requisitoria en ese país.
- ✓ La empresa posee una sede física y legal en el país y la información requerida se encuentra almacenada en servidores locales, pero al ser una empresa extranjera **se rige con la legislación de privacidad de los datos de ese país** y no puede brindar esa información.

Investigación criminal

- ✓ La empresa puede negarse a brindar dicha información por su política de contenidos o de privacidad, aunque estos casos son los menos frecuentes.

Investigación criminal



Quinta dificultad en términos de investigación criminal:

Fragilidad de la evidencia digital:

- ✓ Datos e información digital almacenados o transmitidos en un dispositivo informático que pueden tener validez probatoria para la resolución de un crimen en el marco de una investigación judicial.

Investigación criminal

Características de la evidencia digital:

- ✓ **Inmaterial:** Consta de impulsos eléctricos.
- ✓ **Flexible:** Viajan a la velocidad e la luz y cruzan las fronteras geográficas en segundos.
- ✓ **Volátil:** Se borran automáticamente al apagarse un dispositivo o cerrarse un programa o una aplicación.

Investigación criminal

- ✓ **Anónima:** los archivos digitales generalmente no poseen rasgos personales de un usuario.
- ✓ **Ocultable:** puede almacenarse en unidades de almacenamiento externas (CDs, DVDs, pendrives, tarjetas de memoria, puede ser cifrada (criptografía), guardada en formatos especiales, ocultada dentro de otros archivos (esteganografía) o almacenados con nombres falsos.

Cifra oculta del cibercrimen

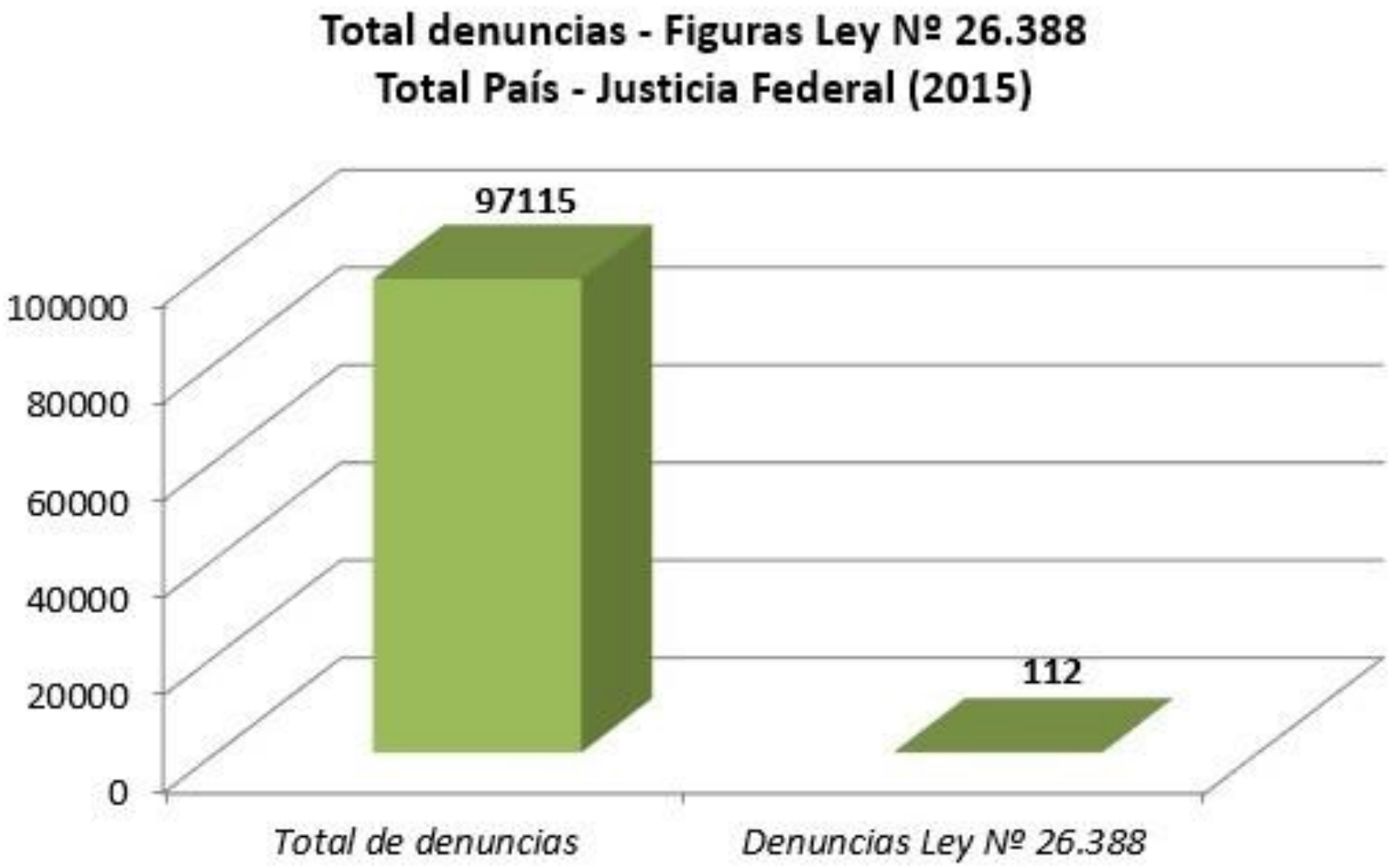
Factores que explican el **bajo nivel de denuncia**:

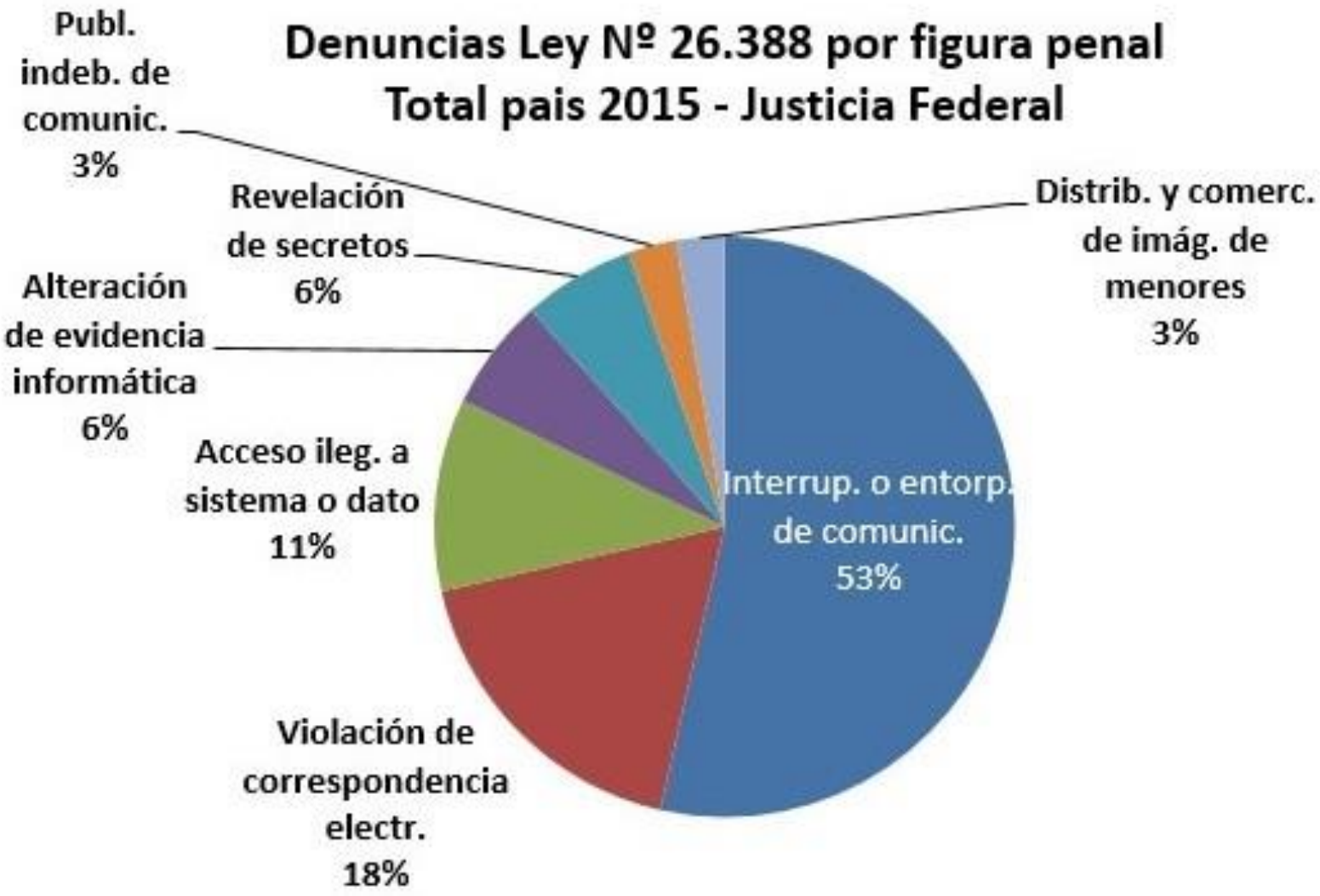
- ✓ Desconocimiento de los usuarios de que están siendo víctimas de un delito.
- ✓ La desconfianza de las víctimas de un delito informatico de que la investigación no va a llegar a una resolución efectiva.
- ✓ Baja resolución judicial (condenas) por dificultades que presenta la investigación criminal de delitos relacionados con dispositivos informáticos.

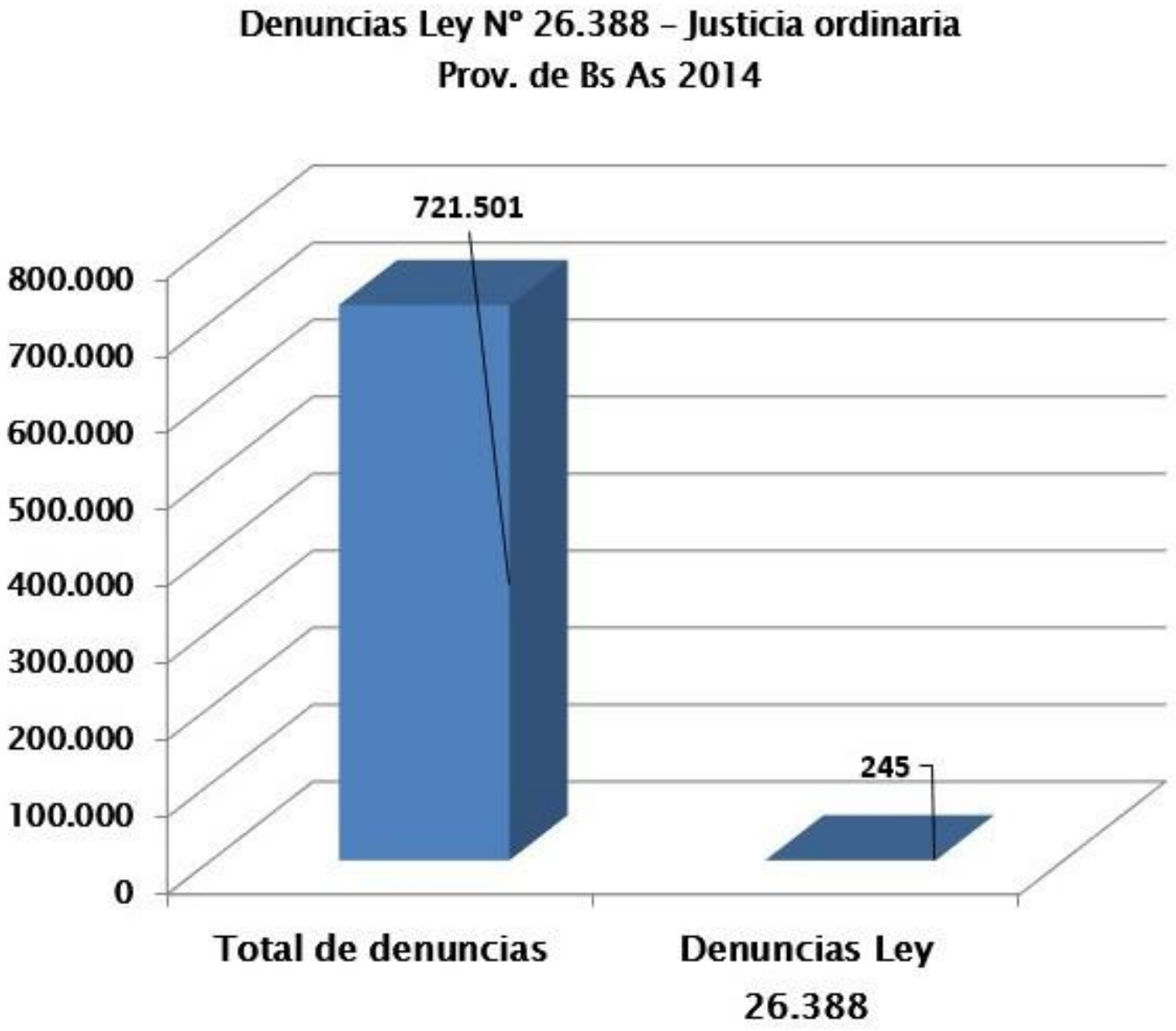
Cifra oculta del cibercrimen

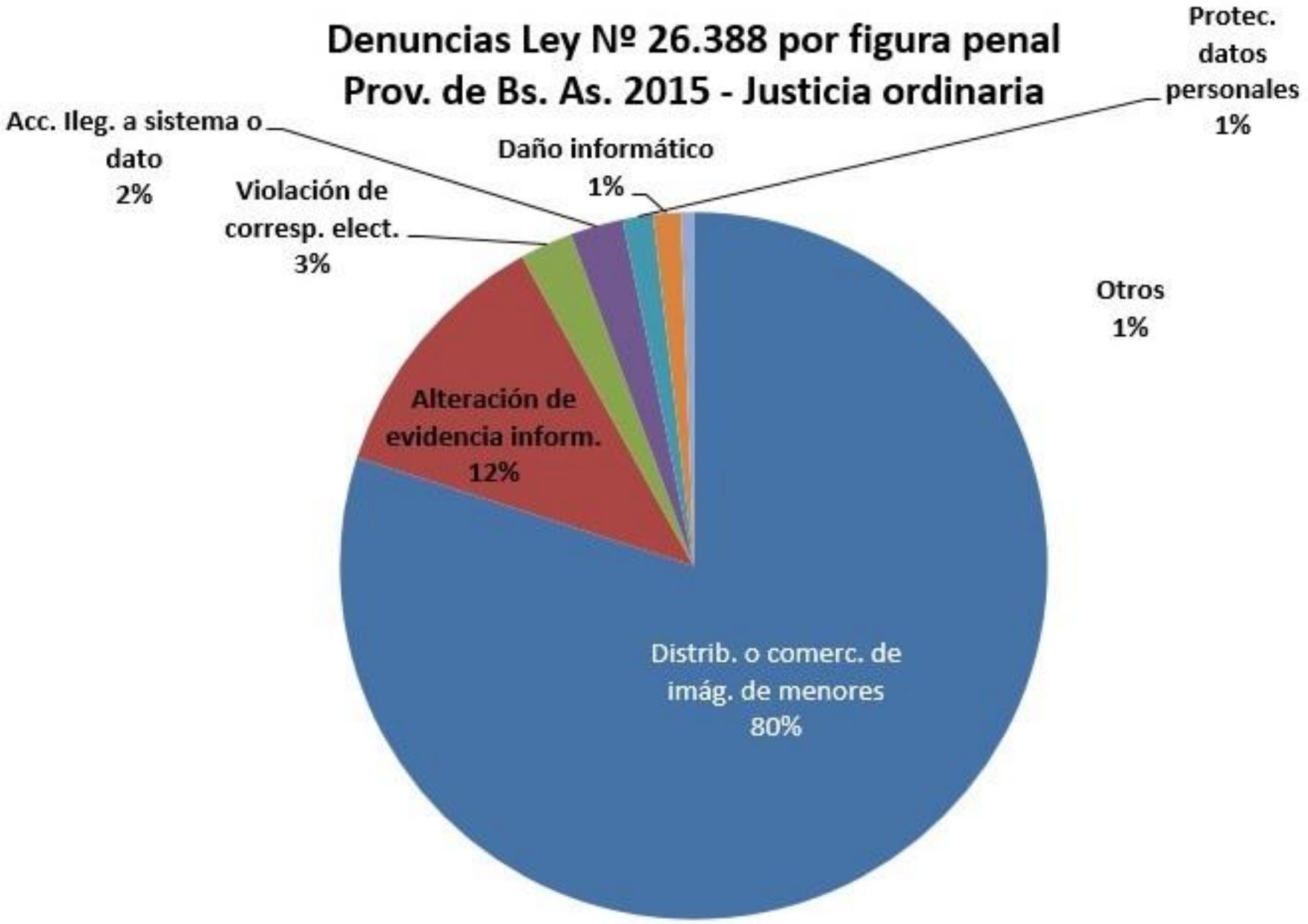
Factores que explican el **bajo nivel de denuncia:**

- ✓ El temor de las empresas a denunciar estos delitos para preservar su imagen y reputación y/o evitar multas o sanciones.
- ✓ Las resoluciones de tipo tecnológicas de estas conductas.
- ✓ Las soluciones administrativas que ofrecen los proveedores de servicio de Internet (ISPs) o empresas que operan en la web.


Total denuncias - Figuras Ley Nº 26.388
Total País - Justicia Federal (2015)
97115
112
100000
80000
60000
40000
20000
0
Total de denuncias
Denuncias Ley Nº 26.388


Denuncias Ley Nº 26.388 por figura penal
Total pais 2015 - Justicia Federal
Publ. indeb. de comunic. 3%
Revelación de secretos 6%
Alteración de evidencia informática 6%
Acceso ileg. a sistema o dato 11%
Violación de correspondencia electr. 18%
Interrup. o entorp. de comunic. 53%
Distrib. y comerc. de imág. de menores 3%


Denuncias Ley Nº 26.388 – Justicia ordinaria
Prov. de Bs As 2014
721.501
245
800.000
700.000
600.000
500.000
400.000
300.000
200.000
100.000
0
Total de denuncias
Denuncias Ley 26.388


Denuncias Ley Nº 26.388 por figura penal
Prov. de Bs. As. 2015 - Justicia ordinaria
Protec. datos personales 1%
Acc. Ileg. a sistema o dato 2%
Daño informático 1%
Violación de corresp. elect. 3%
Otros 1%
Alteración de evidencia inform. 12%
Distrib. o comerc. de imág. de menores 80%

Derecho y cibercrimen

En materia de **prevención de delitos informáticos**:

- ✓ Al igual que la seguridad pública, el derecho i**nterviene cuando la conducta ilícita ya fue cometida.**
- ✓ **No es contra motivacional.**

Derecho y cibercrimen

- La estrategia de **armonización penal** a nivel global para la tipificación de hechos relacionados con dispositivos informáticos presenta ciertas dificultades.
- Cada Estado posee la soberanía política para decidir que conducta es susceptible de recibir una pena y cual no por factores socio-culturales, económicos, etc.

Derecho y cibercrimen

- La **cooperación internacional en materia de derecho procesal penal** depende en la actualidad en la firma de convenios de cooperación judicial entre países y tratados de extradición mas que la adhesión a convenios internacionales como la convención de Budapest

Seguridad informática y cibercrimen

En materia de **prevención de delitos informáticos**:

- La seguridad informática fue pensada para la protección de las redes y los sistemas de las organizaciones en base a las perdidas económicas que pueden producir los ataques informáticos.
- Los Certs no tienen responsabilidad en la investigación de delitos informáticos cometidos en el marco de las organizaciones.

Seguridad informática y cibercrimen

- **La responsabilidad última** de que una persona no sea víctima de un delito informático **es del usuario**.

❖Analogía con una política en materia de seguridad publica:

✓Blindar los domicilios con rejas, cerraduras, alarmas cámaras y el Estado brinde recomendaciones al respecto, intentando penetrarlas para ver el nivel de seguridad de las mismas.

Políticas públicas en Internet

- ✓ Los estados tiene la facultad indelegable de **velar por los derechos y libertades de los ciudadanos**, prioritariamente por la libertad de expresión, el derecho a la información y la privacidad de las comunicaciones.
- ✓ Estos principios no pueden dejarse en manos de las empresas proveedoras de servicios de Internet (ISPs).

Políticas públicas en Internet

¿Como intervenir en una red de comunicaciones con presencia mayoritaria del sector privado sin que los gobiernos vulnere el derecho a la privacidad e intimidad de las personas en términos de prevención ý conjuración delictiva?

Políticas públicas en Internet

Antecedentes:

Directiva sobre Comercio Electrónico de la Unión Europea (2000):

- ✓ Cualquier empresa que brinde servicios económicos de la sociedad de la información en un país de la Unión y ciudadanos de otro país miembro pueden acceder a ellos a través de Internet, se considera que tiene una filial allí.

Políticas públicas en Internet

Ley 12.965 - Marco Civil de Internet en Brasil (2014).

- ✓ Establece los principios básicos de funcionamiento de Internet en el país.
- ✓ Derechos, deberes y garantías de los ciudadanos como usuarios de la red y las empresas proveedoras de servicios, tanto nacionales como extranjeras.

Políticas públicas en Internet

Empresas proveedoras de servicio extranjeras:

- ✓ Deben adecuar los términos y condiciones de uso de sus servicios a la legislación brasileña.
- ✓ Esto se aplica cuando se recolectan datos en territorio brasileño en las comunicaciones o interviene al menos con un dispositivo alojado en ese país.

Políticas públicas en Internet

Prevé una serie de sanciones a las empresas que incumplan con estas disposiciones tales como:

- ✓ Advertencia
- ✓ Multa
- ✓ Suspensión del servicio.
- ✓ Prohibición de actividades.
- ✓ Sin perjuicio de otras sanciones administrativo, civiles o penales.

Políticas públicas en Internet

En términos de **investigación criminal:**

- ✓ Las empresas deben guardar los registros de conexión de sus clientes por el termino de 1 año y los registros de acceso a aplicaciones y servicios por el termino de 6 meses.

Políticas públicas en Internet

- ✓ Las empresas proveedoras de servicio de Internet no tiene responsabilidad civil por los contenidos publicados por terceros.
- ✓ La empresa debe comunicar al usuario que esta violando la ley tras la comunicación de alguna unidad administrativa, después de un plazo estipulado la empresa tiene responsabilidad solidaria sobre el mismo.
- ✓ La empresa solo puede eliminar el contenido de terceros solo mediante orden judicial en caso que sean de índole privadas.

Políticas públicas en Internet

Importancia del **diseño de políticas y estrategias para el desarrollo de Internet** en un país:

- ✓ La existencia de una **ley marco** que delinee los principios básicos de funcionamiento.
- ✓ La creación de un **órgano rector** que establezca las políticas en materia de desarrollo y seguridad de Internet y coordine los organismos competentes en la administración de la red dentro de un país.

Políticas públicas de Internet

Ley marco de Internet en Argentina:

- ✓ Establezca los **derechos y obligaciones** de los usuarios de la red en el país en tanto ciudadanos, no consumidores.
- ✓ Determine claramente el cumplimiento del **derecho a la información, la libertad de expresión y el derecho a la privacidad e intimidad** de las personas en las comunicaciones como principios básicos.

Políticas públicas en Internet

Ley marco de Internet en Argentina:

- ✓ Prohíba **las supervisión y/o monitoreo de comunicaciones privadas** en materia preventiva por parte de las fuerzas de seguridad.
- ✓ Establezca que toda solicitud a los ISPs de registros de personas o comunicaciones se establezca únicamente con **orden judicial**.

Políticas públicas en Internet

Ley marco de Internet en Argentina:

- ✓ **Establezca la adecuación de los términos y condiciones de uso de los servicios** por parte de proveedores de Internet a la legislación de cada país.
- ✓ Establecimiento de **canales de denuncia directa** con organismos de gobierno competentes y sistemas de alerta en sitios web.

Políticas públicas en Internet

Ley marco de Internet en Argentina:

- ✓ Determine la **obligatoriedad** de los administradores de redes de las empresas a **denunciar** a las autoridades competentes cualquier incidentes de seguridad a nivel interno que constituya un delito.

Políticas publicas en Internet

Ley marco de Internet en Argentina:

- ✓ Cree un **organismo central** como ente de aplicación de la ley para el funcionamiento de Internet en el país

Políticas públicas en Internet

Órgano central de Internet:

- ✓ Establezca los **principios básicos de funcionamiento de Internet** en Argentina mediante resoluciones vinculantes:
- ✓ Instrumente estrategias, líneas de acción y políticas de desarrollo técnicas y operacionales.

Políticas públicas en Internet

Órgano central de Internet:

- ✓ Establezca directrices vinculantes de cumplimiento efectivo por parte de proveedores de acceso y servicio de Internet en Argentina, sean empresas locales o extranjeras.
- ✓ Supervise el cumplimiento de la ley marco de Internet en el país.

Políticas públicas en Internet

Órgano central de Internet:

- ✓ Proponga legislación relacionada en materia de ciberseguridad.
- ✓ Realice estudios de tipo criminológicos y estadísticos en materia de cibercrimen.
- ✓ Brinde asesoramiento a organismos de la Administración Publica Nacional, provincial o municipal que así lo requiera.

Políticas públicas en Internet

Órgano central de Internet:

Debe centralizar las funciones de:

- ✓ NIC.ar
- ✓ Programa Nacional de Infraestructuras críticas de la información
- ✓ Área de la Secretaria de TICs del MinMod encargada del registro de proveedores de acceso a Internet
- ✓ Dirección Nacional de Protección de Datos Personales.
- ✓ Comité de Ciberseguridad.

Políticas públicas en Internet

Otras medidas en materia de **seguridad en la red**:

- ✓ Creación de áreas o sectores específicos en organismos públicos para el monitoreo de entornos web públicos de acuerdo a sus competencias.
- ✓ Adecuación de las políticas de privacidad de contenido o seguridad de las empresas a la normativa local y elaboración de reportes periódicos.

Políticas públicas en Internet

Otras medidas en materia de **seguridad en la red**:

- ✓ Establecimiento de protocolos de actuación para las empresas frente a conductas ilícitas o hechos ilegales que se pueden presentar en línea.
- ✓ Creación de legislación específica o actualización de existentes que incluyan las actividades en línea.



Muchas gracias !