

LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL

Aspectos básicos de la criminalidad informática en el nuevo
texto penal tras la reforma por LO 1/2015

JOSE DIAZ CAPPA

FISCAL

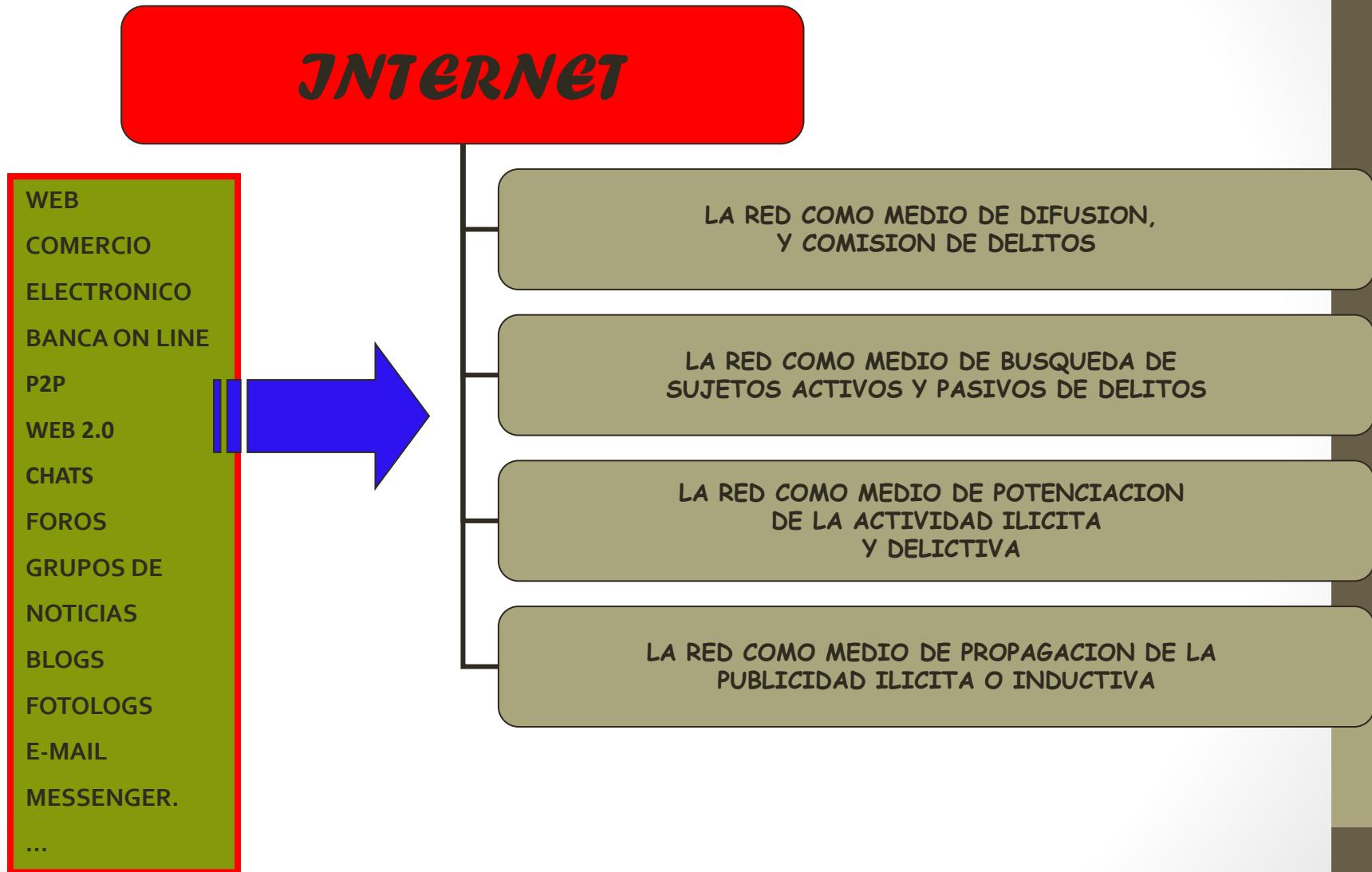
Delegado de Criminalidad Informática. Delegado Sección de Menores.
Delegado Tutela Penal Igualdad y contra la Discriminación. Profesor Asociado UIB

www.josediazcappa.com

jose.diaz@fiscal.es

jose.diaz@uib.eu

el delito en la Red



¿ qué es delito informático?

Convenio Europeo sobre la Ciberdelincuencia

23 noviembre 2001

Contra la
confidencialidad,
integridad y
disponibilidad de
los datos y
sistemas
informáticos.
Hacking.

Delitos de
manipulación
informática.
Phising.

Delitos
informáticos por
contenido.
Pornografía.

Delitos contra la
propiedad
intelectual.
Descargas.

¿qué es delito informático?

Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual

Lanzarote, 25 octubre 2007

Abuso sexual.
prostitución
infantil.
Pornografía
infantil.
Espectáculos
pornográficos.
Corrupción

Complicidad y
tentativa.
Personas
Jurídicas.
Agravantes.

Competencia.

Investigación,
enjuiciamiento
y Cooperación
Internacional.

2. A) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.

-Delitos de daños, sabotaje informático y ataques de denegación de servicios previstos y penados en el artículo 264 y concordantes del Código Penal.

-Delitos de acceso sin autorización a datos, programas o sistemas informáticos previstos y penados en el artículo 197.3 del Código Penal.

-Delitos de descubrimiento y revelación de secretos del artículo 197 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

-Delitos de descubrimiento y revelación de secretos de empresa previstos y penados en el artículo 278 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos.

-Delitos contra los servicios de radiodifusión e interactivos previstos y penados en el artículo 286 del Código Penal.

2. B) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.

-Delitos de estafa previstos y penados en el artículo 248.2 a) b) y c) del Código Penal, siempre que, en los supuestos a) y c) se utilicen las TICs para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

-Delitos de acoso a menores de 13 años, *child grooming*, previstos y penados en el art. 183 bis del Código Penal cuando se lleve a efecto a través de las TICs.

-Delitos de corrupción de menores o de personas discapacitadas o relativas a pornografía infantil o referida a personas discapacitadas previstos y penados en el artículo 189 del Código Penal cuando para el desarrollo y/o ejecución de la actividad delictiva se utilicen las TICs.

-Delitos contra la propiedad intelectual de los artículos 270 y ss del Código Penal cuando se cometan utilizando las TICs.

2. C) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña especial complejidad en su investigación que demanda conocimientos específicos en la materia.

-Delitos de falsificación documental de los artículos 390 y ss del Código Penal cuando para la ejecución del delito se hubieran empleado las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad técnica en la investigación criminal.

-Delitos de injurias y calumnias contra funcionario público, autoridad o agente de la misma previstos y penados en los artículos 211 y ss del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de amenazas y coacciones previstos y penados en los artículos 169 y ss del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos contra la integridad moral previstos y penados en el artículo 173.1 del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio previstos y penados en los artículos 510 y 607.2 del Código Penal cometidos a través de las TICs siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs y en los que dicha circunstancia genere una especial complejidad en la investigación criminal.

CIBERDELITOS ECÓNICOS O PATRIMONIALES

ESTAFA

Artículo 248.

1. Cometan estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

INGENIERÍA SOCIAL

INGENIERÍA SOCIAL

FRAUDE
ONLINE

ENGAÑO (PICA EL
ANZUELO)

ERROR (DAME TUS DATOS)

PERJUICIO (ADIOS TU
DINERO)

INGENIERÍA SOCIAL

SPAM



HOAX



SCAM



FALSOS PERFILES

VIRUS



SMShing, Vising, Wishing



Carding



Phising, pharming



GOBIERNO
DE ESPAÑA



CUERPO
NACIONAL
DE POLICIA

Fue detectado un caso de actividad ilegal. El sistema oper

Desde su dirección IP bajo el número [REDACTED] fue efectuado un ac
menores. En su ordenador asimismo fueron encontrados archivos de vídeo q
realizaba envío de spam con subtexto de terrorismo. El

ransomware

Your details:
[REDACTED]

**Para quitar el bloqueo del ordenador, usted debe pagar
una multa de 100 euro.**

Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad
junto con la contraseña) en la línea del pago, y posteriormente pulse OK
(si usted tiene varios códigos, intodúzcalos uno detrás de otro, y
después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo
electrónico deposito@cyber-police.net.

PHISING

Obtención de datos, claves, contraseñas, números de tarjetas mediante engaño y con ánimo de lucro.

- *Engaño, ánimo de lucro, error en otro y perjuicio.*

PHISING

- **SERVIDORES PARA PHISING (RBN: russian business network)**
- **Alertas bancarias.**
- **EL TROYANO ZEUS (falsifica extractos bancarios)**
- **Las tarjetas de coordenadas y los snniffers.**
- **Uso de “tarjetas calientes”**

Smishing



Dear client, we require you to send the first and second OTP numbers you received on your phone via SMS to 07#7216365. This is required by the South African Police to verify your bank account that is attached to your mobile phone number. You will be prosecuted if you don't send it immediately. Send the 2 OTP numbers to 07#7216365.

El Smishing, (Phishing a través de SMS), consiste en el envío de SMS a teléfonos móviles con el fin de obtener información privada de los usuarios. Las prisas y el temor son los peores aliados de este usuario, que, en la precipitación y la necesidad de dar una respuesta rápida a un problema que parece urgente, realiza el envío de los datos solicitados.

PHARMING

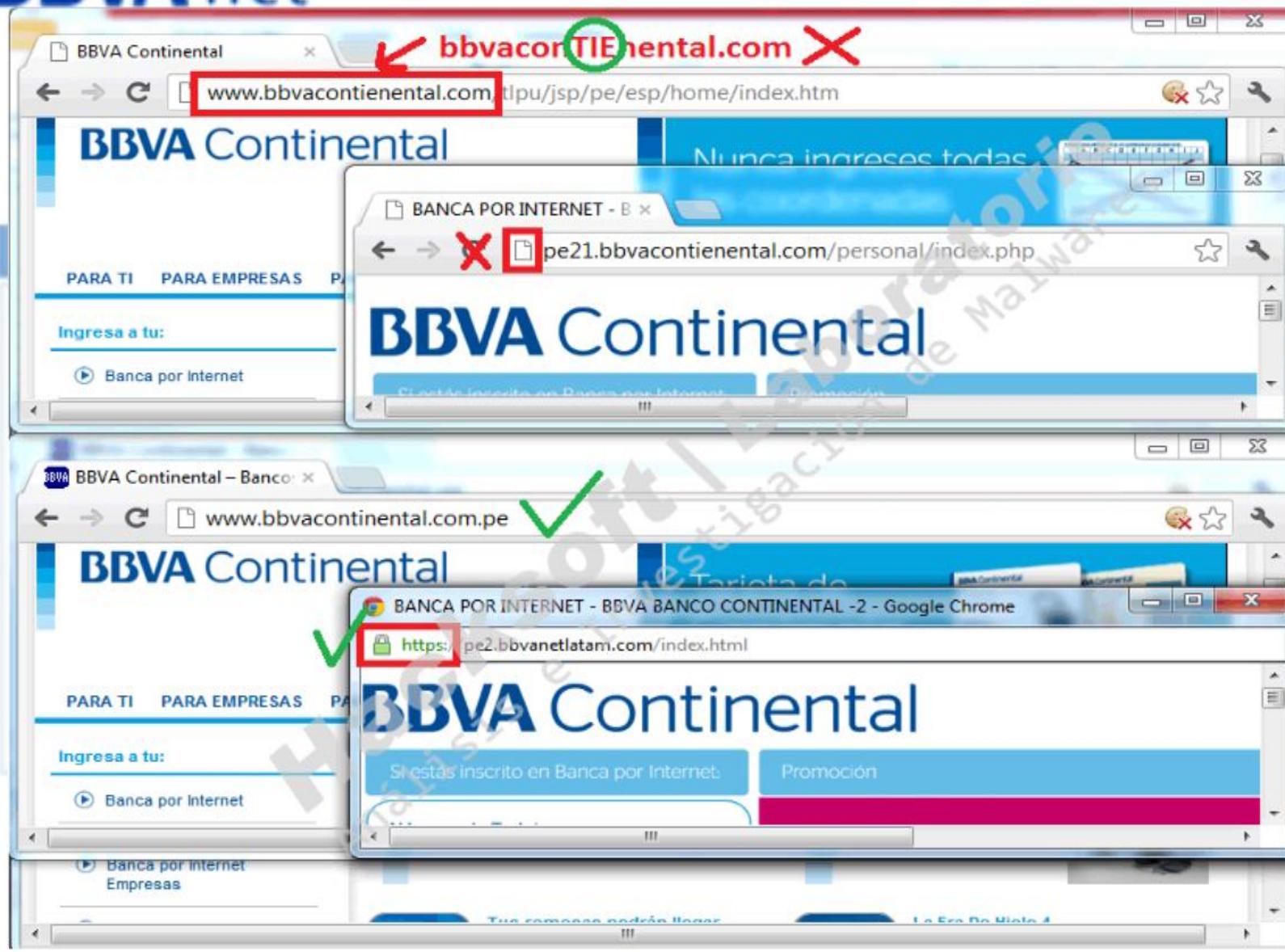
REDIRECCIONAMIENTO DE NOMBRES DE DOMINIO. Recreación y simulación de páginas web reales.

- Se ataca el DNS o el fichero hosts que lo pueda contener en la memoria del equipo.

APROPIACION DIRECCION IP ASOCIADA AL NOMBRE DE DOMINIO

**FINALIDAD : LA MISMA QUE EL PHISING.
PÁGINAS DE IMITACION: WEB SPOOFING**

BBVA net



Hotmail - Tuenti

www.tuenti.com.msg1.es/?m=login

Phishing

 **tuenti**

¿Qué es Tuenti?

Tuenti es una plataforma social privada, a la que se accede únicamente por invitación. Cada día la usan millones de personas para comunicarse entre ellas y compartir información.

Email Contraseña

Recordarme [Has olvidado tu contraseña?](#)

[Entrar](#)

 **Social**
Conéctate, comparte y comunícate con tus amigos, compañeros de trabajo y familia.

 **Local**
Descubre servicios locales y participa con las marcas que realmente te importan.

 **Móvil**
Accede a Tuenti desde tu móvil en tiempo real estés donde estés.

© Tuenti 2011 Castellano Català English Euskara Galego

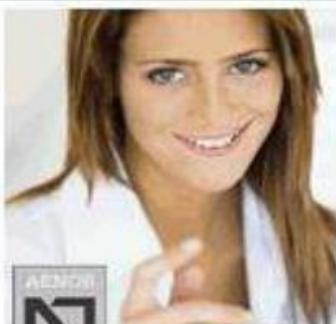
Acerca de Empleo Anúnciate Prensa Blog Desarrolladores Ayuda Legal

Páginas oficiales: 



Acceso a Banca por Internet

Los clientes que van a responder correcto a las 3 preguntas , van a entrar a una tombola. Usted puedes ser uno de los felices ganadores . Le pedimos los siguiente datos para saber donde vamos a mandar los 1500,00 EUR si usted va a ser uno de los ganadores de este mes.



Primer banco español
con certificado
AENOR de Calidad de
Servicio

Tipo de documento:

Número de documento:

Código de usuario:

Clave personal:

Clave de Firma:



Aceptar

pharming

BBVA

Particulares
B. Privada | Negocios | Empresas

Acceso cliente / área privada

usuario:
contraseña:

¿Has olvidado tu contraseña?
[Entrar](#)

Acceso con DNI electrónico

Todavía no eres usuario de bbva.es? Solicita tu acceso:
[Alta usuario](#)

Gana premios por utilizar **bbva.es**

Si ya lo conoces, juega desde la parte privada de **bbva.es**

[Conoce BBVA game](#)

BBVA game

te ayudamos a...

Gestionar el día a día Ahorrar / Invertir Obtener Financiación Vivir más tranquilo Buscar Casa Ir de Compras

NBA

descubre a tu nuevo...
Asesor BBVA Contigo

Consulta también > Banca Personal > Jóvenes > Mayores > Extranjeros

Síguenos en: [f](#) [t](#) [b](#)

BBVA - Particulares - Windows Internet Explorer

Http://www.bbva.seguridad.net/www/TBSL/bbva/particulares/

Archivo Edición Ver Historial Ayuda

Favoritos BBVA - Particulares

BBVA

Particulares
B. Privada | Negocios | Empresas

Acceso cliente / área privada

usuario:
contraseña:

Alta,olvidado.tu.contraseña
[Entrar](#)

Acceso con DNI electrónico

Comienza a operar en BBVA.es

Dale de alta ahora y aprovecha los vantajes de ser usuario de BBVA.es.

Aunque no seas cliente, también podrás utilizar varios servicios de esta web. Y, por supuesto, podrás darte de alta como cliente.
[Alta usuario](#)

Cada día nos pides algo diferente. Cada día somos un banco diferente.

hoy nos pides...

Gestionar mi día a día Ahorrar / Invertir Obtener Financiación Vivir más tranquilo Ir de Compras Buscar Casa

Consulta también > Jóvenes > Mayores > Extranjeros

PROMOCIONES

BBVA DESDE CUALQUIER LUGAR

E-mail Seguridad | Aviso legal | Tarifas y otros avisos | Mapa | Atención al cliente | Banco Bilbao Vizcaya Argentaria S.A. - 2010

Internet 100%

¿Qué deseas buscar?

PHISER-MULERS

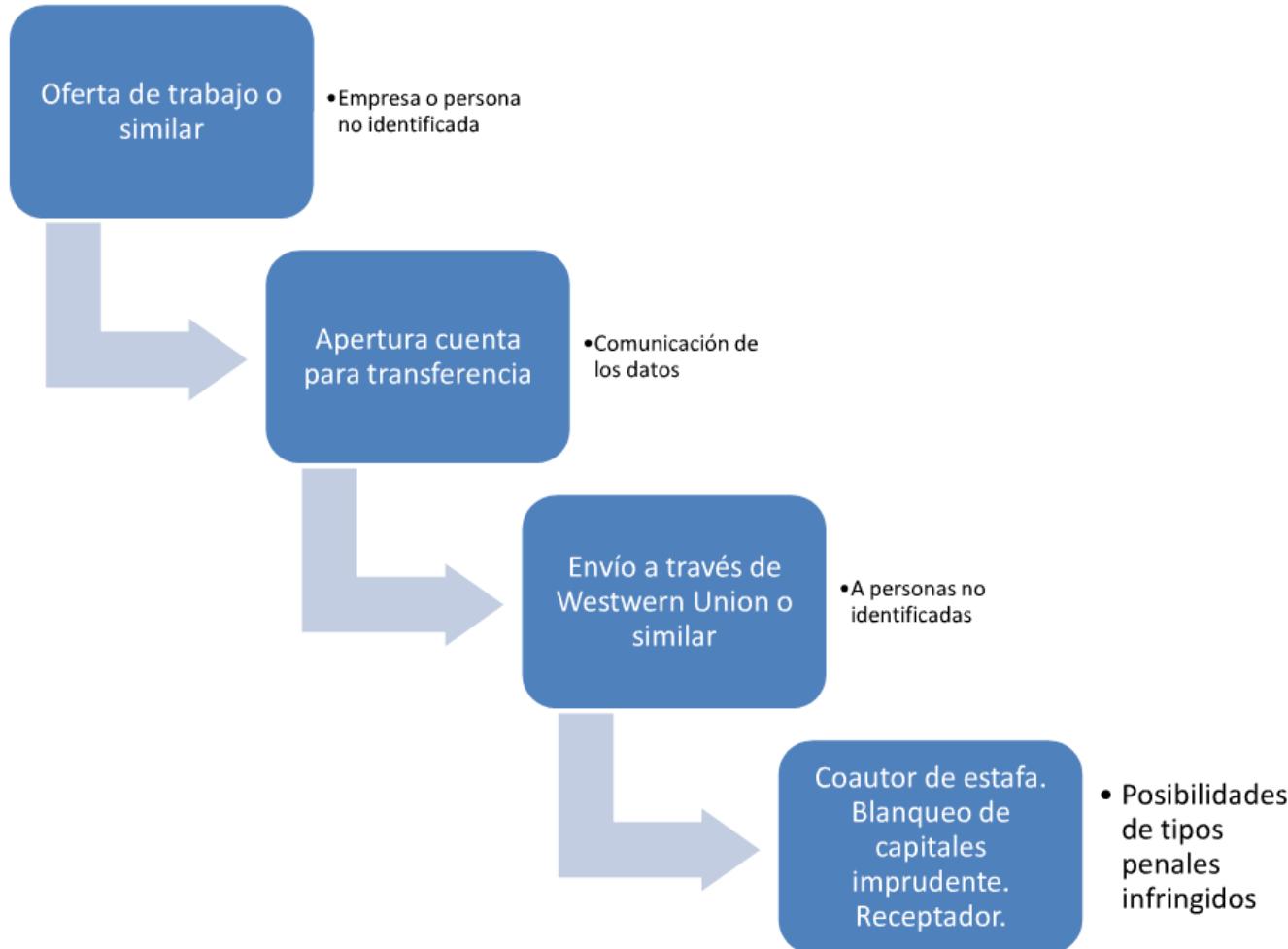
• BLANQUEO DE CAPITALES IMPRUDENTE

Artículo 301.

1. El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triple del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años.

3. Si los hechos se realizasen por imprudencia grave, la pena será de prisión de seis meses a dos años y multa del tanto al triple.

Proceso del “mulero” en internet



DEFRAUDACIÓN DE TELECOMUNICACIONES

Artículo 255.

1. Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1.^º Valiéndose de mecanismos instalados para realizar la defraudación.

2.^º Alterando maliciosamente las indicaciones o aparatos contadores.

3.^º Empleando cualesquiera otros medios clandestinos.

2. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

DEFRAUDACIÓN DE TELECOMUNICACIONES

Artículo 256.

1. El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico, será castigado con la pena de multa de tres a doce meses.

2. Si la cuantía del perjuicio causado no excediere de 400 euros, se impondrá una pena de multa de uno a tres meses.

DAÑOS INFORMÁTICOS

cracking

Artículo 264.

1. El que por cualquier medio, sin autorización y de manera grave borrarse, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.^a Se hubiese cometido en el marco de una organización criminal.

2.^a Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.^a El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.^a Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.^a El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

DAÑOS INFORMÁTICOS

Artículo 264 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

- a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

DAÑOS INFORMÁTICOS

denegación de servicio DoS

Artículo 264 bis.

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

- a) realizando alguna de las conductas a que se refiere el artículo anterior; |
- b) introduciendo o transmitiendo datos; o
- c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

daños en hardware y software

**ping de la
muerte**

sniffers

**puertas
traseras**

smurfing

**bombas
lógicas**

bacterias

troyanos

**worms
(gusanos)**

bugs

Propiedad intelectual

Artículo 270.

1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicaamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

Propiedad intelectual

Se
puede
acordar

retirada

interrupción

bloqueo

otras medidas

Propiedad intelectual

“Top manta”

Artículo 270.

4. En los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 271, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

Propiedad intelectual

(otras conductas)

Artículo 270.

5. Serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes:

- a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente.
- b) Importen intencionadamente estos productos sin dicha autorización, cuando estuvieran destinados a ser reproducidos, distribuidos o comunicados públicamente, tanto si éstos tienen un origen lícito como ilícito en su país de procedencia; no obstante, la importación de los referidos productos de un Estado perteneciente a la Unión Europea no será punible cuando aquellos se hayan adquirido directamente del titular de los derechos en dicho Estado, o con su consentimiento.
- c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización.
- d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.

6. Será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo.

Propiedad industrial

patentes y modelos de utilidad

Artículo 273.

1. Será castigado con la pena de prisión de seis meses a dos años y multa de 12 a 24 meses el que, con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio objetos amparados por tales derechos.

2. Las mismas penas se impondrán al que, de igual manera, y para los citados fines, utilice u ofrezca la utilización de un procedimiento objeto de una patente, o posea, ofrezca, introduzca en el comercio, o utilice el producto directamente obtenido por el procedimiento patentado.

3. Será castigado con las mismas penas el que realice cualquiera de los actos tipificados en el párrafo primero de este artículo concurriendo iguales circunstancias en relación con objetos amparados en favor de tercero por un modelo o dibujo industrial o artístico o topografía de un producto semiconductor.

Propiedad industrial

marcas

Artículo 274.

1. Será castigado con las penas de uno a cuatro años de prisión y multa de doce a veinticuatro meses el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro,

a) fabrique, produzca o importe productos que incorporen un signo distintivo idéntico o confundible con aquel, u

b) ofrezca, distribuya, o comercialice al por mayor productos que incorporen un signo distintivo idéntico o confundible con aquel, o los almacene con esa finalidad, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

2. Será castigado con las penas de seis meses a tres años de prisión el que, con fines industriales o comerciales, sin consentimiento del titular de un derecho de propiedad industrial registrado conforme a la legislación de marcas y con conocimiento del registro, ofrezca, distribuya o comercialice al por menor, o preste servicios o desarrolle actividades, que incorporen un signo distintivo idéntico o confundible con aquél, cuando se trate de los mismos o similares productos, servicios o actividades para los que el derecho de propiedad industrial se encuentre registrado.

La misma pena se impondrá a quien reproduzca o imite un signo distintivo idéntico o confundible con aquél para su utilización para la comisión de las conductas sancionadas en este artículo.

3. La venta ambulante u ocasional de los productos a que se refieren los apartados anteriores será castigada con la pena de prisión de seis meses a dos años.

No obstante, atendidas las características del culpable y la reducida cuantía del beneficio económico obtenido o que se hubiera podido obtener, siempre que no concurra ninguna de las circunstancias del artículo 276, el Juez podrá imponer la pena de multa de uno a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días.

Propiedad industrial

(otras conductas)

También títulos de obtención vegetal
se castiga

denominación de origen o una
indicación geográfica representativa

divulgación de la invención objeto de
una solicitud de patente secreta

Secretos de empresa

“contra el mercado y los consumidores”

Artículo 278.

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Artículo 279.

La difusión, revelación o cesión de un secreto de empresa llevada a cabo por quien tuviere legal o contractualmente obligación de guardar reserva, se castigará con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

Si el secreto se utilizara en provecho propio, las penas se impondrán en su mitad inferior.

Artículo 280.

El que, con conocimiento de su origen ilícito, y sin haber tomado parte en su descubrimiento, realizare alguna de las conductas descritas en los dos artículos anteriores, será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses.

falsedades

Spoofing:
falsificación documentos informáticos
(arts. 390 y ss)

alteración, copia, reproducción o de
cualquier otro modo falsificación de
tarjetas de crédito o débito o
cheques de viaje
(399 bis)

Blanqueo de capitales

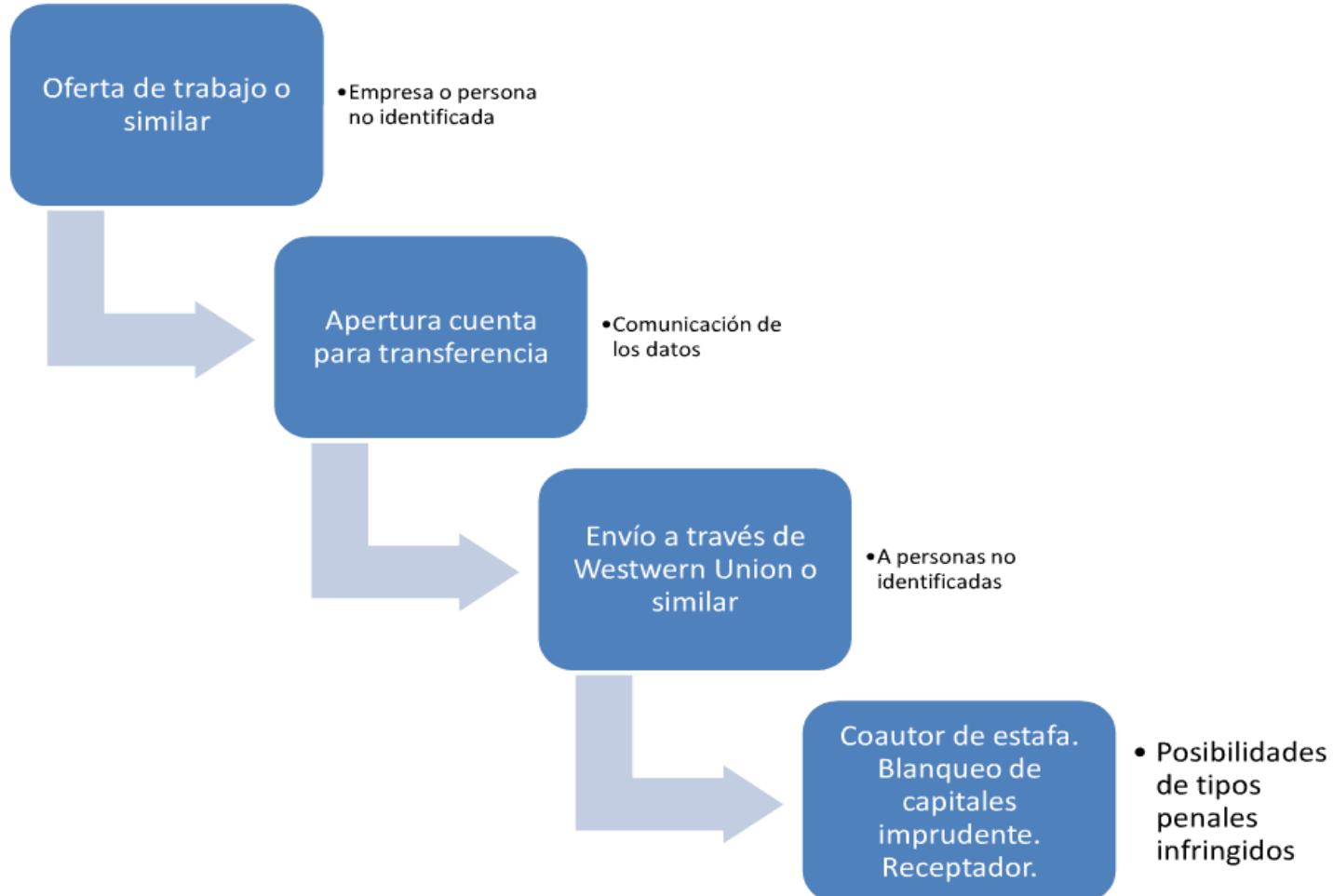
(imprudente)

Artículo 301.

1. El que adquiera, posea, utilice, convierta, o transmita bienes, sabiendo que éstos tienen su origen en una actividad delictiva, cometida por él o por cualquiera tercera persona, o realice cualquier otro acto para ocultar o encubrir su origen ilícito, o para ayudar a la persona que haya participado en la infracción o infracciones a eludir las consecuencias legales de sus actos, será castigado con la pena de prisión de seis meses a seis años y multa del tanto al triple del valor de los bienes. En estos casos, los jueces o tribunales, atendiendo a la gravedad del hecho y a las circunstancias personales del delincuente, podrán imponer también a éste la pena de inhabilitación especial para el ejercicio de su profesión o industria por tiempo de uno a tres años, y acordar la medida de clausura temporal o definitiva del establecimiento o local. Si la clausura fuese temporal, su duración no podrá exceder de cinco años.

3. Si los hechos se realizasen por imprudencia grave, la pena será de prisión de seis meses a dos años y multa del tanto al triple.

Proceso del “mulero” en internet



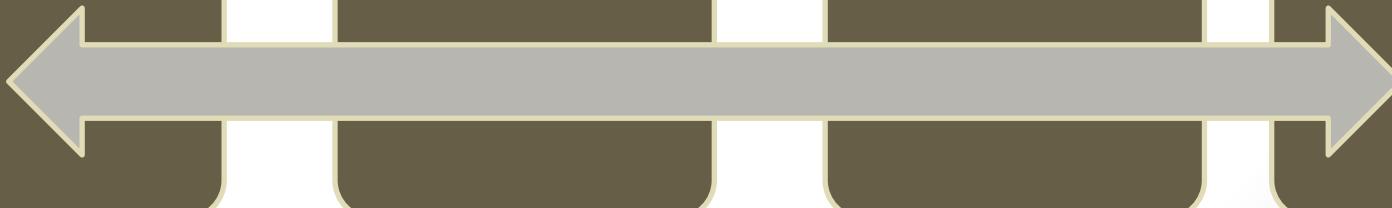
Ciberdelincuencia contra menores

Child-grooming

sexting

Ciberbullying

Pornografía.
Corrupción
de menores.



Recordando...

CP

189 (pornografía)

183 ter (*childgrooming*)

189 y 197 (*sexting*)

173.1 (integridad moral,
ciberbullying)

child grooming

Artículo 183 ter.

1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

2. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

integridad moral

Artículo 173.

1. El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral, será castigado con la pena de prisión de seis meses a dos años.

Pornografía infantil

Conductas
(189 CP)

Uso, captación

Distribución, compartir

Posesión, acceso

Asistencia a actos

Stalking (acoso)

Artículo 172 ter.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.^a La vigile, la persiga o busque su cercanía física.

2.^a Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.^a Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.^a Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

Quebrantamiento de condena

Artículo 468.

1. Los que **quebrantaren su condena, medida de seguridad, prisión, medida cautelar, conducción o custodia** serán castigados con la pena de prisión de seis meses a un año si estuvieran privados de libertad, y con la pena de multa de doce a veinticuatro meses en los demás casos.
2. Se impondrá en todo caso la pena de prisión de seis meses a un año a los que quebrantaren una pena de las contempladas en el artículo 48 de este Código o una medida cautelar o de seguridad de la misma naturaleza impuesta en procesos criminales en los que el ofendido sea alguna de las personas a las que se refiere el artículo 173.2, así como a aquellos que quebrantaren la medida de libertad vigilada.
3. Los que **inutilicen o perturben el funcionamiento normal de los dispositivos técnicos** que hubieran sido dispuestos para controlar el cumplimiento de penas, medidas de seguridad o medidas cautelares, no los lleven consigo u omitan las medidas exigibles para mantener su correcto estado de funcionamiento, serán castigados con una pena de multa de seis a doce meses.

Delitos contra la intimidad

(descubrimiento de secretos)

conductas básicas

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Igualas penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Delitos contra la intimidad

(descubrimiento de secretos)

revelar, difundir o ceder

Artículo 197.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

Delitos contra la intimidad

(descubrimiento de secretos)

tipos cualificados

Artículo 197.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

Delitos contra la intimidad

(descubrimiento de secretos)

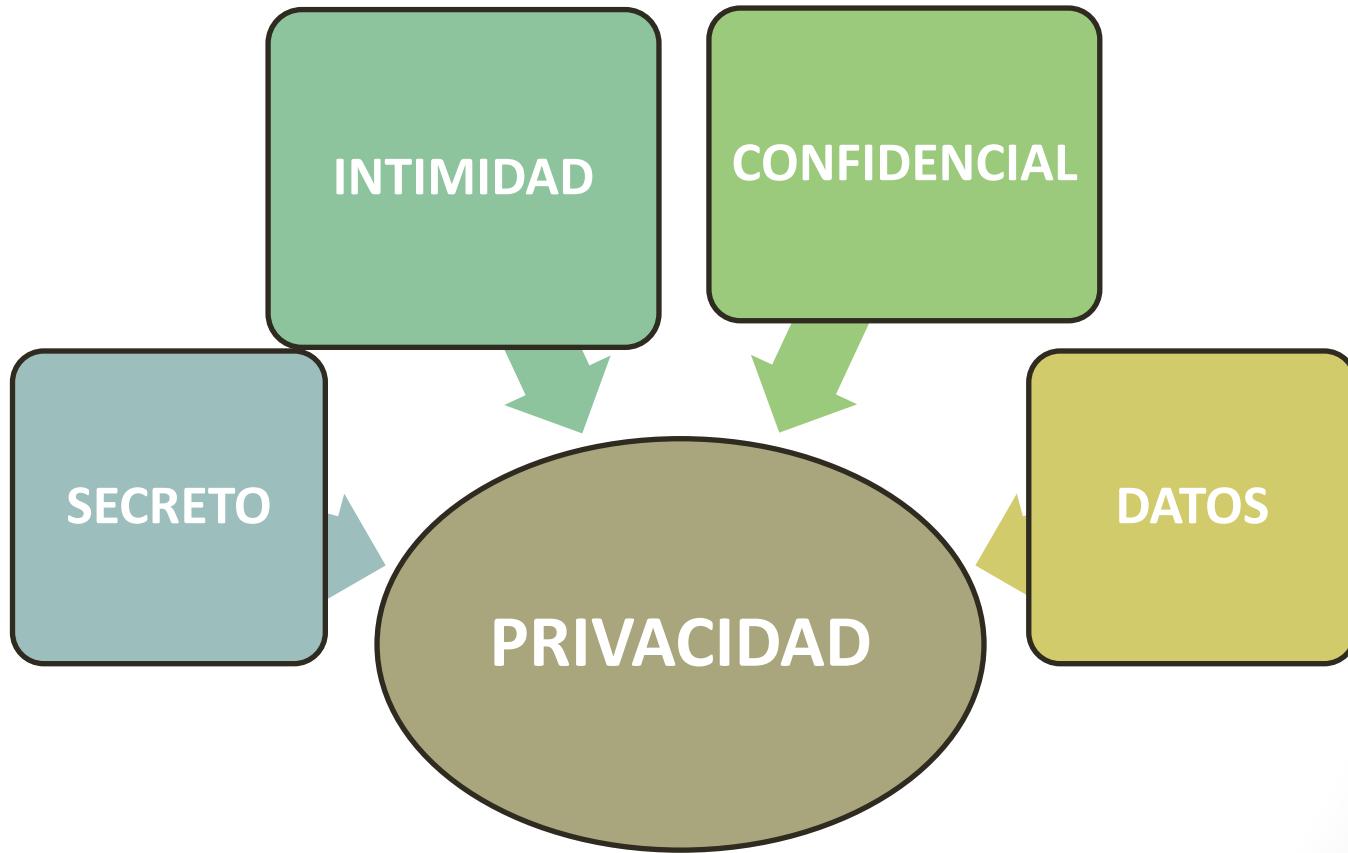
datos obtenidos inicialmente con consentimiento

Artículo 197.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

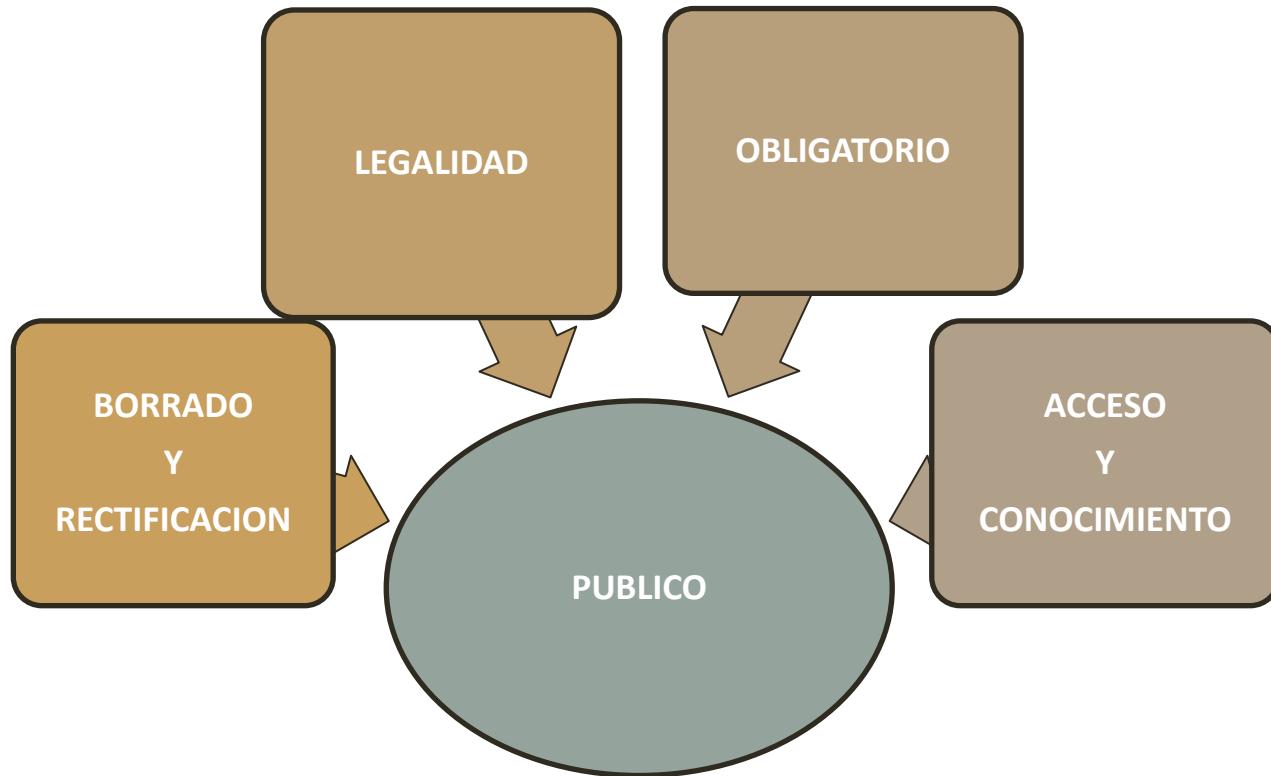
La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

PRIVADO



PREVENCION

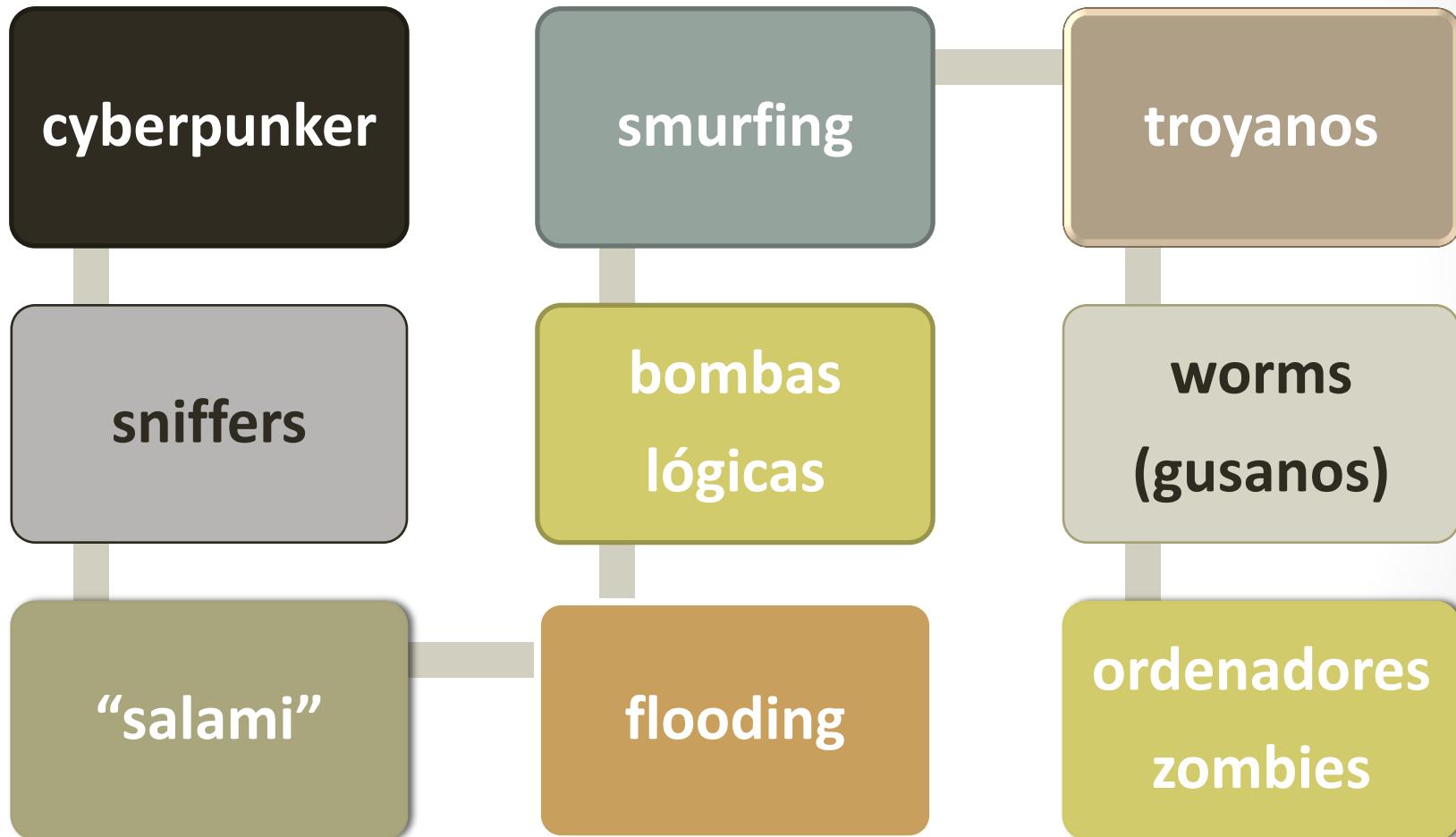
PUBLICO



SEGURIDAD

Internet e intimidad

"me meto en tu ordenador"



Redes sociales



- Perfiles abiertos
- Configuración de privacidad
- Menores
- Indexación y búsqueda de personas.
- Compartir o sólo ver fotos y datos
- Responsabilidad de lo que publicas sobre tí y de lo que publicas sobre los demás. Responsabilidad del riesgo ajeno.
- Redes sociales personales y profesionales.
- La ENISA, Agencia Europea de Seguridad de las Redes y de la Información.

Suplantación de identidad perfiles falsos

- No existe como tipo penal autónomo
“suplantación de identidad”

JUEVES, 22 de abril de 2010

Alejandro Sanz denuncia que en Twitter suplantan su identidad

■ El cantante advierte a sus fans de que ponen en su boca mensajes racistas - Un falso Will Smith circula en la red

MÁBEL GALAZ | Madrid | 22 ABR 2010

Archivado en: Twitter Declaraciones prensa Alejandro Sanz Tecnología Gente Empresas Economía Sociedad


Alejandro Sanz es víctima de una campaña que intenta desprestigiarle a través de la red social Twitter. Así lo ha contado el propio cantante en un mensaje. "Están falsificando twitters míos, como si yo los escribiera haciéndome ver como racista. Ya me avisó Juanes que a él le hicieron lo mismo".


Los ataques han comenzado hace un par de días por los mensajes que Alejandro Sanz ha dejado en Twitter en los que critica a Hugo Chávez. "El Gobierno de Hugo Chávez utiliza niños como guerrilla comunicacional... Es despreciable y lamentable que la comunidad internacional no haga nada" o "señores del Gobierno de Venezuela utilizar a los niños políticamente es la cobardía y la ruindad más grande que he visto en toda mi vida" o "bloqueo a tod@s los chavistas... Inviten a l@s fans de tod@s los artistas a hacerlo".

Los problemas han comenzado tras Algunos seguidores del cantante

KIOSKO y más

Formato PDF enriquecido

SECCIONES

- PRIMERA
- INTERNACIONAL
- ESPAÑA
- ECONOMÍA
- OPINIÓN
- VIÑETAS
- SOCIEDAD
- CULTURA
- TENDENCIAS

GENTE

- OBITUARIOS
- DEPORTES
- PANTALLA
- ÚLTIMA

EDICIONES

- ANDALUCÍA
- CATALUÑA
- C. VALENCIANA
- GALICIA
- MADRID
- PAÍS VASCO

SUPLEMENTOS

- CIBERPAÍS
- QUADERN CATALUNYA



“suplantación de identidad”

POR [PORTADA](#) » [EMPRESAS](#)

El Corte Inglés es suplantado a través de varias cuentas de Twitter

ALVARO MOHORTE. *10/01/2012* La cadena de grandes almacenes tiene cinco perfiles a su nombre en la red de microblogs, aunque asegura que no gestiona ninguno de ellos

[imprimir](#) | [enviar a un amigo](#)

■ COMPARTE ESTA NOTICIA

Twittear

0

VALENCIA. La denuncia del nuevo fiscal general del Estado, **Eduardo Torres-Dulce**, por una suplantación de su identidad en la red social **Twitter** es sólo un caso destacado, pero no extraño



Delitos contra la intimidad

(descubrimiento de secretos)

allanamiento informático

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Delitos contra la intimidad

(descubrimiento de secretos)

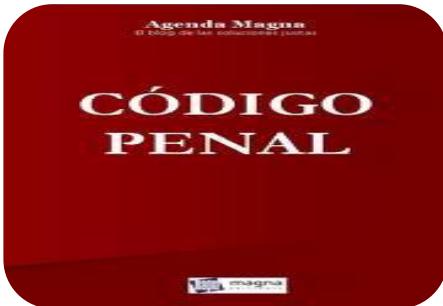
facilitación de la comisión de los delitos anteriores

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

- a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Fórmulas legales de protección



**PROTECCIÓN
PENAL**



**PROTECCIÓN
CIVIL**

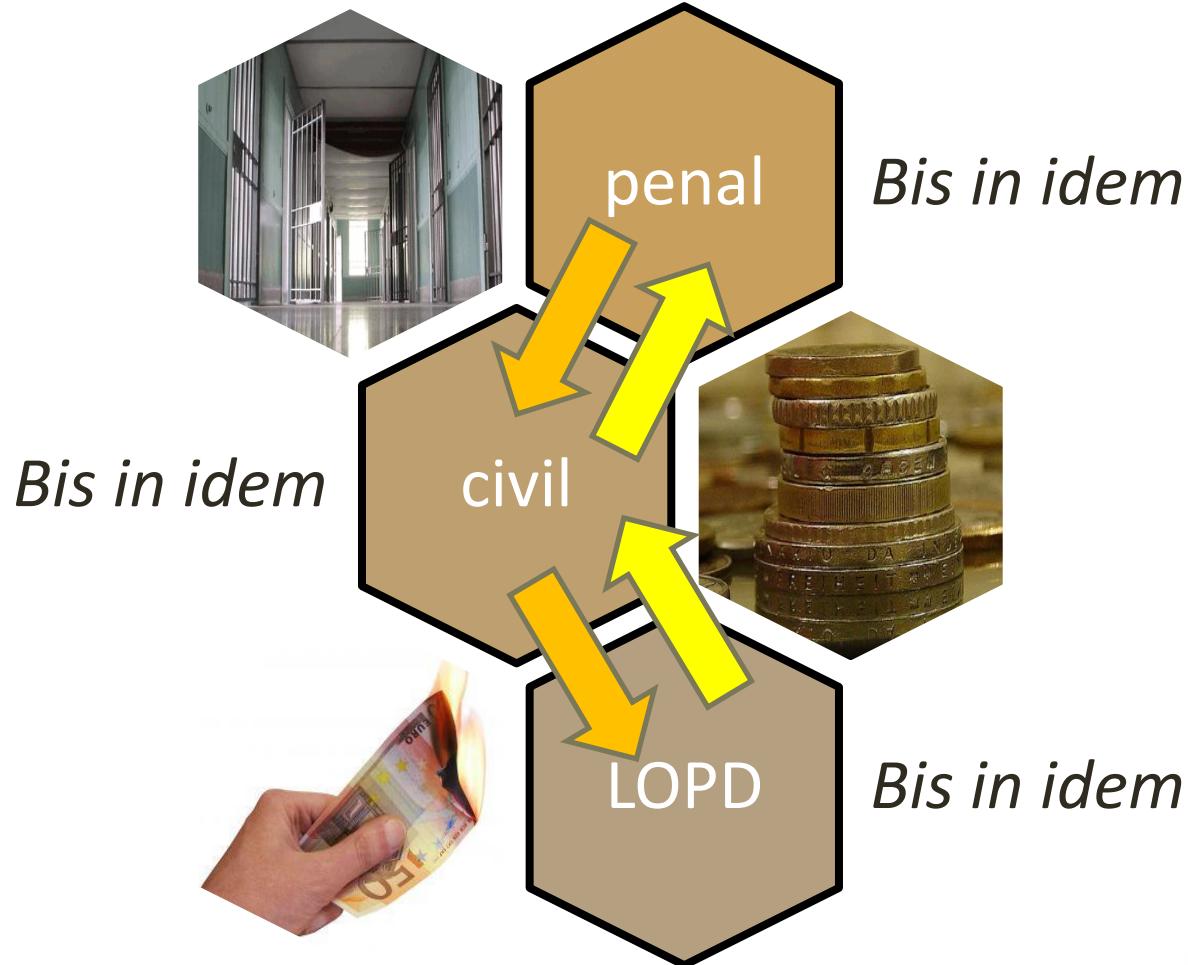


**PROTECCIÓN
ADMINISTRATIVA**



RESPONSABILIDAD

Responsabilidades solapadas



Cloud computing



Fuente: google imágenes y microsoft.com

Cloud computing



Fuente: google imágenes y microsoft.com

Cloud computing



Fuente: google imágenes y blog-idee/blogspot.com

Otros posibles delitos informáticos

calumnias

injurias

orden público (559, 560 CP)

“Delitos de odio”

- FOMENTO, PROMOCIÓN O INCITACIÓN AL ODIO O DISCRIMINACIÓN, DISTRIBUCIÓN DIFUSIÓN O VENTA DE MATERIAL A ELLO DESTINADO, NEGACIÓN O TRIVIALIACIÓN DE DELITOS DE GENOCIDIO O LESA HUMANIDAD, ETC, QUE SE CONVIERTEN EN TIPO CUALIFICADO SI...
- “...los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas”.
- **Art. 510 cp**

Artículo 510.

1. Serán castigados con una pena de prisión de uno a cuatro años y multa de seis a doce meses:

- a) Quienes **públicamente fomenten, promuevan o inciten directa o indirectamente al odio, hostilidad, discriminación o violencia** contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.
- b) Quienes **produzcan, elaboren, posean con la finalidad de distribuir, faciliten a terceras personas el acceso, distribuyan, difundan o vendan escritos o cualquier otra clase de material o soportes que por su contenido sean idóneos para fomentar, promover, o incitar directa o indirectamente al odio, hostilidad, discriminación o violencia** contra un grupo, una parte del mismo, o contra una persona determinada por razón de su pertenencia a aquél, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad.
- c) **Públicamente nieguen, trivialicen gravemente o enaltezcan los delitos de genocidio, de lesa humanidad o contra las personas y bienes protegidos en caso de conflicto armado, o enaltezcan a sus autores**, cuando se hubieran cometido contra un grupo o una parte del mismo, o contra una persona determinada por razón de su pertenencia al mismo, por motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, la situación familiar o la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad, **cuando de este modo se promueva o favorezca un clima de violencia, hostilidad, odio o discriminación contra los mismos.**

terrorismo

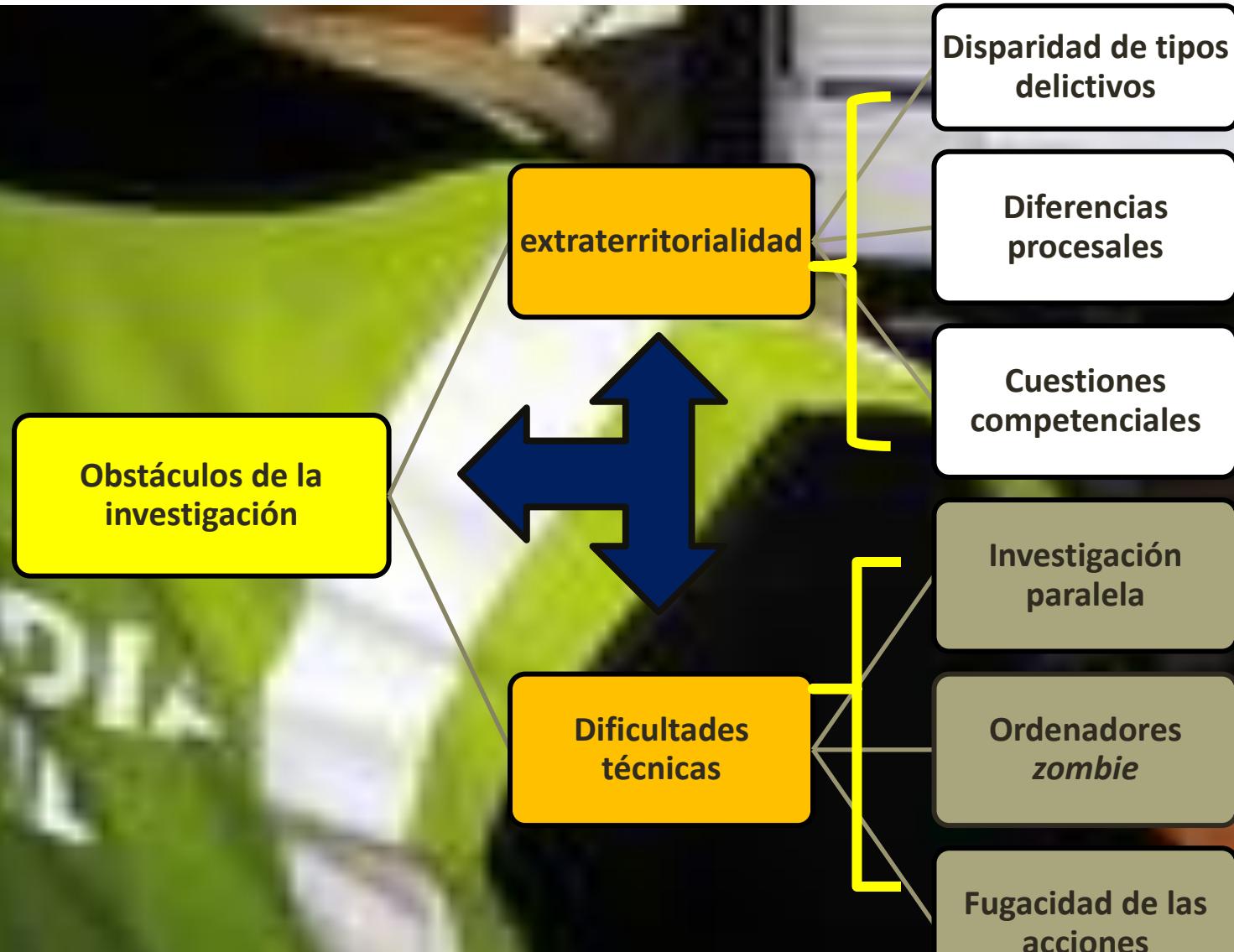
ejemplos ciberataques

apología (578)

adoctrinamiento (575.2)

difusión consignas o mensajes (579)

Algunos aspectos procesales de la criminalidad informática



TEORIA DE LA UBICUIDAD

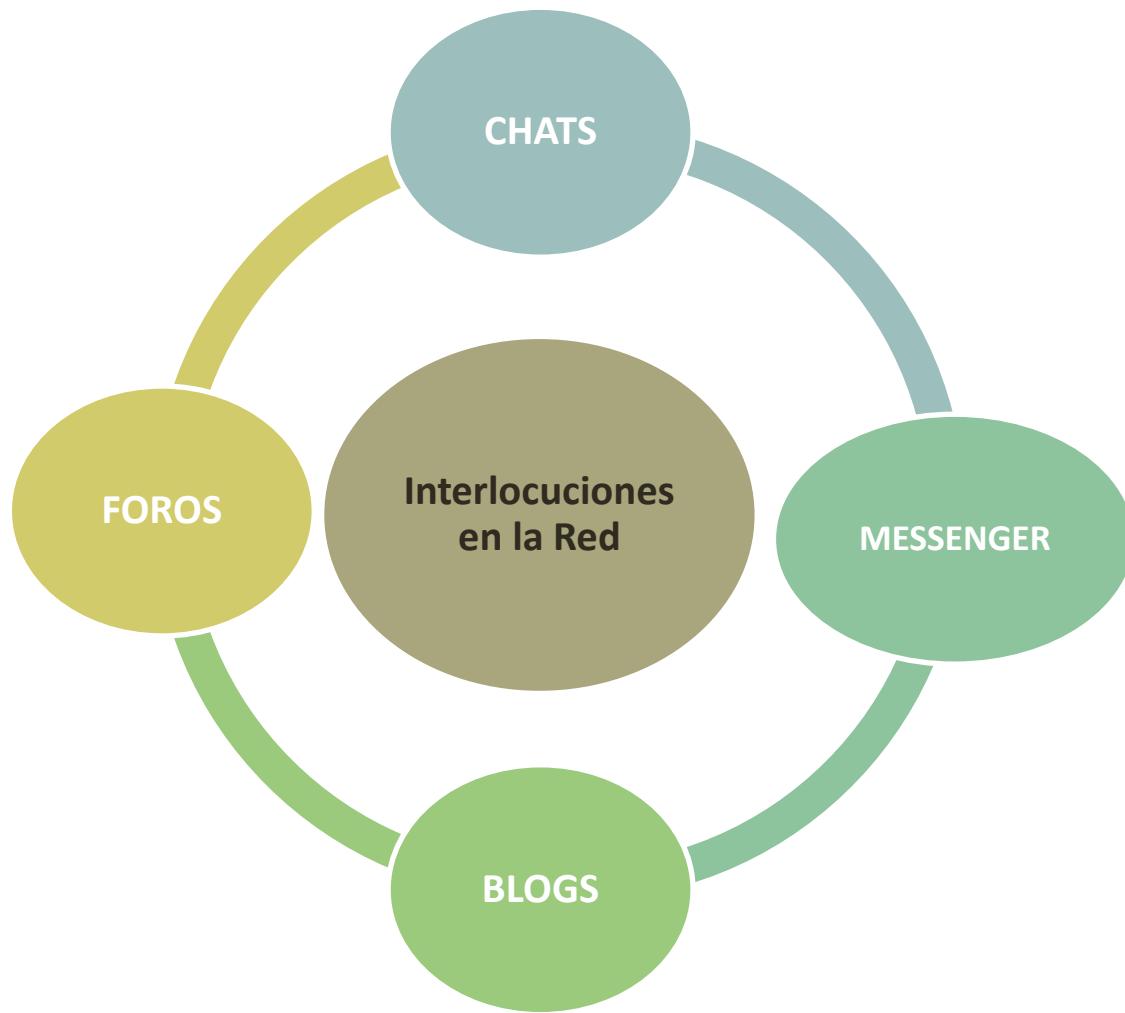
Acuerdo del Pleno no jurisdiccional de la Sala Segunda, adoptado en su reunión del día 3-2-05

PRINCIPIO DE UBICUIDAD.- ACUERDO: "EL DELITO SE COMETE EN TODAS LAS JURISDICCIONES EN LAS QUE SE HAYA REALIZADO ALGÚN ELEMENTO DEL TIPO. EN CONSECUENCIA, EL JUEZ DE CUALQUIERA DE ELLAS QUE PRIMERO HAYA INICIADO LAS ACTUACIONES PROCESALES, SERÁ EN PRINCIPIO COMPETENTE PARA LA INSTRUCCIÓN DE LA CAUSA".-

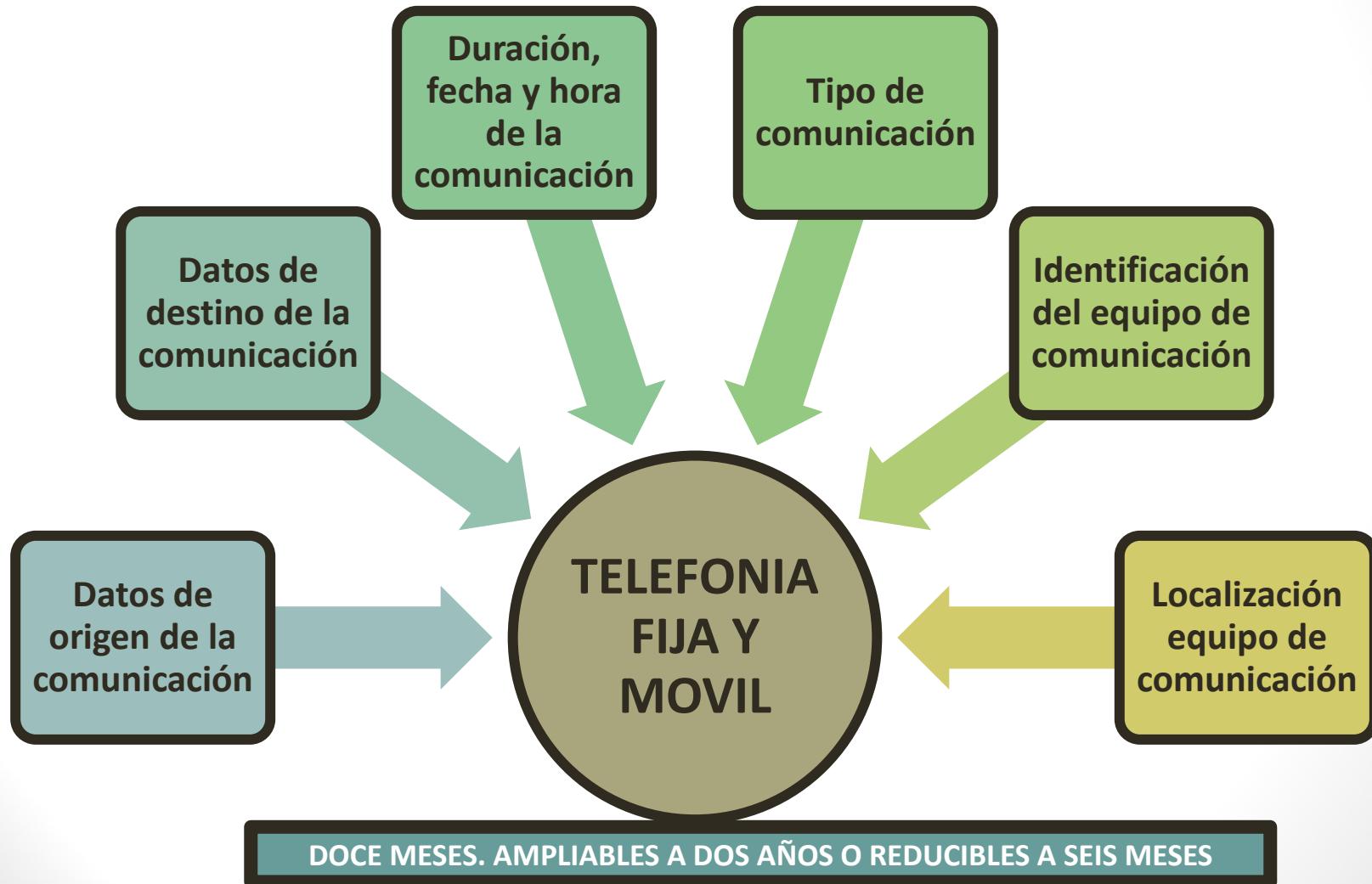
Derechos fundamentales y comunicaciones en la red



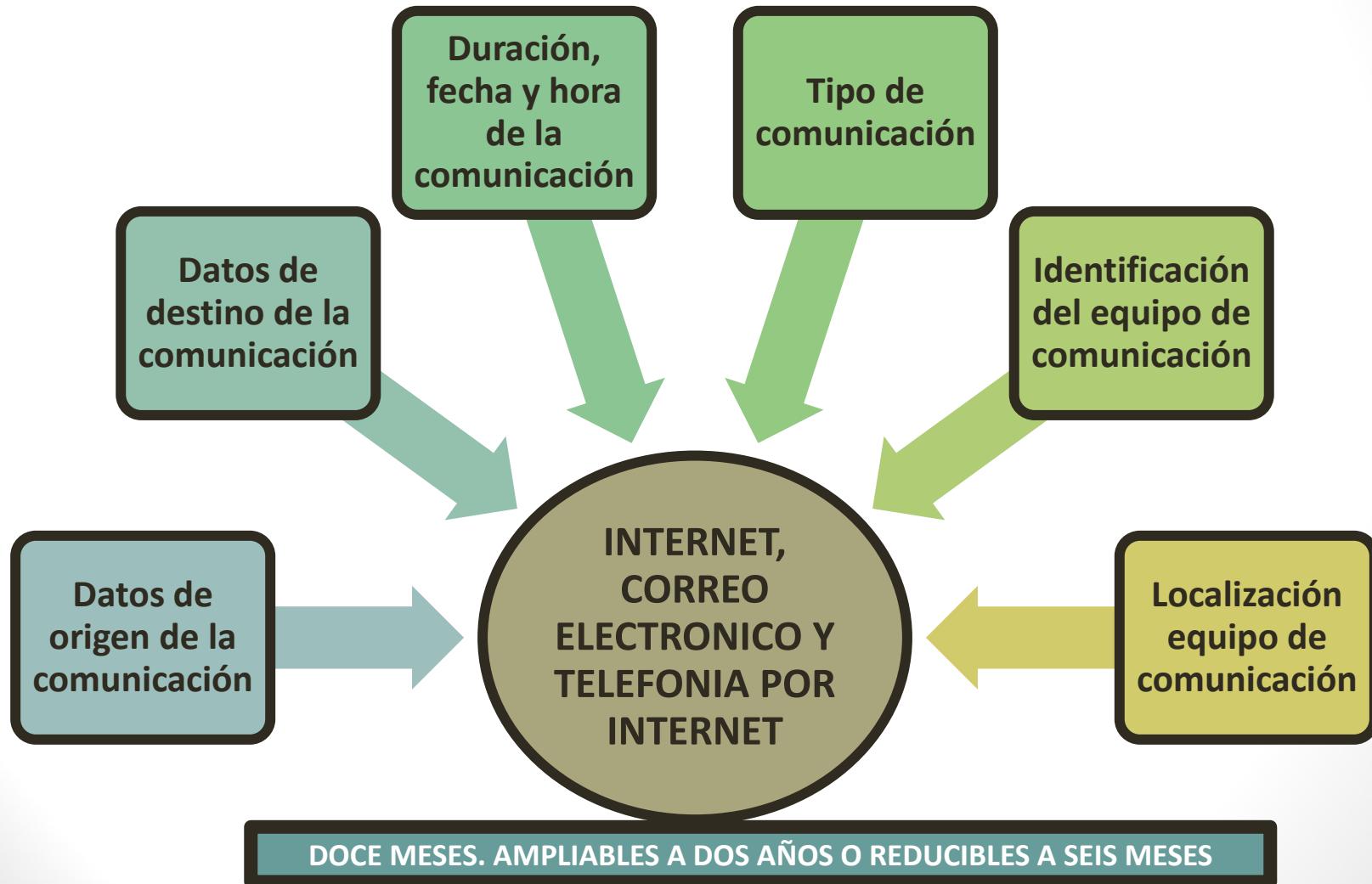
Derechos fundamentales y conversaciones en la red



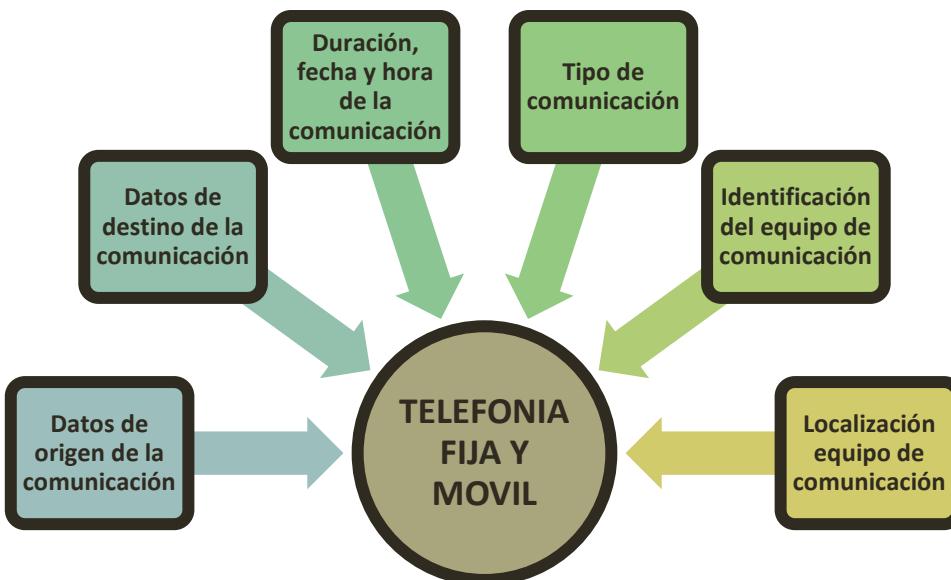
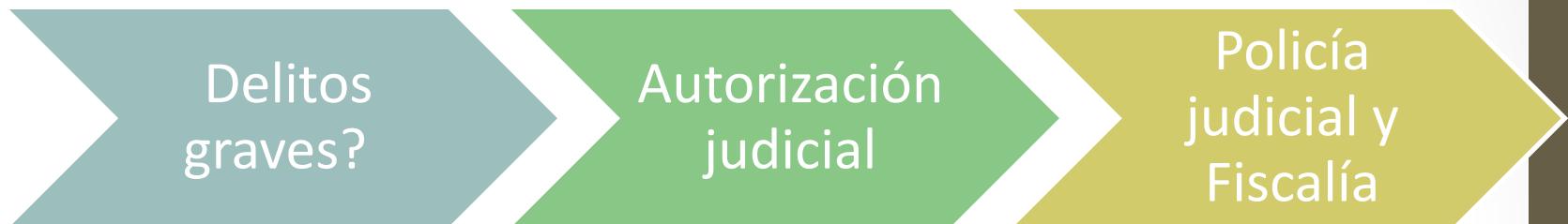
**LEY 25/2007 DE 18 DE OCTUBRE, DE CONSERVACIÓN DE DATOS
RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS Y A LAS REDES
PÚBLICAS DE COMUNICACIONES**



LEY 25/2007 DE 18 DE OCTUBRE, DE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS Y A LAS REDES PÚBLICAS DE COMUNICACIONES



LEY 25/2007 DE 18 DE OCTUBRE, DE CONSERVACIÓN DE DATOS RELATIVOS A LAS COMUNICACIONES ELECTRÓNICAS Y A LAS REDES PÚBLICAS DE COMUNICACIONES



mecanismos de colaboración internacional



INTERPOL



EUROPOL (intercambio de información policial)

- EUROJUST (unidad de cooperación judicial)
- CEPOL (formación policial)



**CONVENIOS ASISTENCIA JURIDICA INTERNACIONAL EN MATERIA PENAL.
SCHENGEN. BILATERALES.**

- Tramitaciones urgentes. Persecución “en caliente”
- Equipos policiales de investigación conjunta
- Investigaciones encubiertas.
- Vigilancia transfronteriza.
- Intervención de telecomunicaciones. (L. 25/07 18 de octubre, conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones)
- Intercambio policial de datos.
- Comunicación directa entre autoridades judiciales.
- Información sentencias extranjeras (RD95/09, 6 febrero, sobre sistema de registros administrativos de apoyo a la Administración de Justicia)

Alguna cuestiones relacionadas con los medios de investigación



Alguna cuestiones relacionadas con la prueba



Técnicas de investigación

- En redes abiertas
- Agente encubierto
- Pericia de inteligencia policial
- Geolocalización
- softwares

LA INCORPORACION DE LA PRUEBA AL PROCESO PENAL

- MISMAS GARANTIAS QUE PARA CUALQUIER OTRO SUPUESTO SIMILAR: selección judicial; cotejos, etc ...
 - DOCUMENTAL
 - PERICIAL:
 - Testigos peritos
 - Periciales técnicas
 - Policía Judicial
 - Policía Científica.

El juicio de inferencia

- **ST JUZGADO PENAL 3 PALMA 11 de octubre de 2010:**
- “*no ha quedado acreditado que el material descargado a través del programa Emule fuera objeto de difusión a otros usuarios por voluntad expresa del acusado y no de modo automático o por defecto, como es propio de dicho programa de intercambio*”.
- “*trece archivos resulta un número pequeño y despreciable para deducir de ello la voluntad de difundir*”
- **Pleno no Jurisdiccional TS 27 octubre 2009:** “*una vez establecido el tipo objetivo del art. 189.1.b) del CP, el subjetivo deberá ser considerado en cada caso, evitando incurrir en automatismos derivados del mero uso del programa informático empleado para la descarga de archivos*”

Reforma LECRIM intervenciones telemáticas

LINEAS BÁSICAS DE LA REFORMA

NO PROSPECTIVAS

**SOBRE EQUIPOS USADOS HABITUAL U
OCASIONALMENTE**

CARÁCTER SUBSIDIARIO

**TRES AÑOS, ORGANIZACIÓN O DELITOS
COMETIDOS A TRAVES DE TIC**

Reforma LECRIM intervenciones telemáticas

LINEAS BÁSICAS DE LA REFORMA



COMUNICACIONES Y DATOS DE TRAFICO

PETICION Y CONTENIDO

OBLIGACION DE COLABORACIÓN PRESTADORES Y PROVEEDORES Y PARTICULARES. DESOBEDIENCIA

AMPLIACION DEL REGISTRO PJ Y MF

Reforma LECRIM intervenciones telemáticas

LINEAS BÁSICAS DE LA REFORMA



USO ARTIFICIOS TECNICOS POR PJ PARA IDENTIFICACIÓN DE USUARIOS,
TERMINALES Y DISPOSITIVOS DE CONECTIVIDAD

GRABACIÓN DE COMUNICACIONES ORALES DIRECTAS

AGENTE ENCUBIERTO INFORMÁTICO PODRA INTERCAMBIAR O ENVIAR
POR SI MISMO ARCHIVOS ILÍCITOS Y ANALISIS DE SUS ALGORITMO

Reforma LECRIM intervenciones telemáticas

LINEAS BÁSICAS DE LA REFORMA



**ENTRADA Y REGISTRO AUTO
HABILITANTE A EQUIPOS**

**OCUPACION EXTRADOMICILIARIA
DE EFECTOS INFOMÁTICOS**

**REGISTROS REMOTOS SOBRE
ELEMENTOS INFORMÁTICOS**

LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL

Aspectos básicos de la criminalidad informática en el nuevo
texto penal tras la reforma por LO 1/2015

JOSE DIAZ CAPPA

FISCAL

Delegado de Criminalidad Informática. Delegado Sección de Menores.
Delegado Tutela Penal Igualdad y contra la Discriminación. Profesor Asociado UIB

www.josediazcappa.com

jose.diaz@fiscal.es

jose.diaz@uib.eu