



Dirección General de la Mujer
CONSEJERÍA DE POLÍTICAS SOCIALES
Y FAMILIA

Comunidad de Madrid

**MIÉRCOLES 31 DE
ENERO DE 2018**

JORNADA FORMATIVA

**ASPECTOS LEGALES DE LA VIOLENCIA DE GÉNERO.
CUESTIONES CONCRETAS: MENORES, TECNOLOGÍA Y
SEGUNDA OPORTUNIDAD**

Alejandro Sánchez del Campo
@replicantelegal

Los delitos tecnológicos después de la reforma del Código Penal de 2015

1. Delito de intrusión informática (artículo 197 bis apartado primero).

"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 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. Interceptación de transmisiones de datos informáticos (artículo 197 bis apartado segundo)

“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”.

3. Delitos informáticos relacionados con la propiedad intelectual e industrial (artículos 270 y ss CP)

"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 económicamente, 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.

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".

4. Otro tipo de delitos informáticos

Algunos no son más que subtipos o submodalidades de delitos ya existentes (como las amenazas, injurias, calumnias) cuya comisión se produce valiéndose de las nuevas tecnologías; mientras que en otros supuestos estamos ante nuevos tipos penales.

Sin ánimo exhaustivo, podemos citar:

- .-amenazas (**artículo 169 y ss del CP**) realizadas o difundidas a través de cualquier medio de comunicación.
- .-calumnias e injurias (**artículo 205 y ss CP**) realizadas o difundidas a través de cualquier medio de comunicación.
- .-fraudes informáticos (**artículo 248 del CP**)
- .-sabotaje informático (**artículo 263 del CP**)
- .-inducción a la prostitución de menores (**artículo 187**)
- .-producción, venta, distribución, exhibición o posesión de material pornográfico en cuya elaboración hayan intervenido o sido utilizados menores de edad o incapaces (**artículo 189 CP**)
- .-posesión de software informático destinado a cometer delitos de falsedad .
- .-cualesquiera otros delitos de descubrimiento o revelación de secretos (**artículo 197 y ss**)

Poniendo más el foco en violencia de género

- Se incluye un nuevo delito de acoso, acecho u hostigamiento (stalking) mediante llamadas telefónicas continuas, seguimientos o cualquier otra fórmula que pueda lesionar gravemente la libertad y el sentimiento de seguridad de la víctima, aunque no se produzca violencia (Art. 172 ter CP)
- Se tipifica como nuevo delito la divulgación no autorizada de grabaciones o imágenes íntimas obtenidas con el consentimiento de la víctima, pero luego divulgadas sin que ésta lo sepa, cuando afecten gravemente a su intimidad (*sexting*).

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.

Art. 197.7 CP

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.

De esta forma, se acaba con la impunidad reinante antes de la modificación del Código Penal, ya que en su antigua redacción no se recogían este tipo de conductas, por lo que, se está dando respuesta a actuaciones de indudable gravedad que en muchas ocasiones, no podían ser calificadas como coacciones o amenazas (en el caso del “stalking”) o que meramente eran calificadas como un ilícito civil de intromisión ilegítima en el derecho al honor (en el caso del “sexting”).

La prueba en el caso de delitos tecnológicos

Artículo 3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, por la cual, se considerará “documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”.

No hay duda (ahora) de que esos documentos se pueden aportar en juicio (evidencias electrónicas)

¿Cómo se aporta en juicio una evidencia electrónica?

La aportación como prueba de un correo electrónico o mensaje de WhatsApp o se podrá efectuar mediante un acta notarial en la cual se constatará por el Notario la existencia de dichos mensajes, otorgando fe pública del acceso a la cuenta de correo o del dispositivo móvil donde esté instalada la aplicación de mensajería, y procediendo a imprimir los mensajes elegidos incorporándolos finalmente al acta notarial.

En el acta de “protocolización” de los mensajes normalmente se incluye también la dirección de correo electrónico o el número de teléfono desde los que se hayan enviado o recibido los mensajes, las fechas de los referidos mensajes, así como las identidades de los intervinientes que figuren en los textos protocolizados.

El mismo valor probatorio de documento público tendrán las diligencias realizadas en el propio Juzgado a petición de los interesados (fe pública judicial). En este caso, será el Letrado de la Administración de Justicia el que levante acta del contenido del concreto correo electrónico o mensaje de WhatsApp, identidades que figuren en dichos mensajes, así como del dispositivo móvil utilizado.

La Policía también puede hacerlo en el momento de la denuncia

Adicionalmente a las anteriores fórmulas de aportación de pruebas electrónicas, y como un plus de garantía de autenticidad y no manipulación, se presenta la posibilidad de practicar una prueba pericial informática sobre el contenido de los mensajes electrónicos, y en general sobre cualquier otro contenido almacenado digitalmente, como pueden ser ordenadores, dispositivos móviles, páginas webs, redes sociales o similares.

¿Por qué es importante la intervención del perito informático?

Los Notarios no tienen conocimientos técnicos ni pueden dar fe de lo que no ven o perciben por los sentidos

La prueba electrónica es fácilmente alterable.

Existe multitud de información asociada con nuestros documentos electrónicos, que se pierden en la impresión y que pueden ayudarnos a la hora de conseguir una valoración adecuada de la prueba (metadatos).

En contra, es caro.



Why Metadata Matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

Mail

Sergio Carrasco Mayans <sergioc@derechonntt.com>

11 de abril de 2016, 19:31

Para: d.sergiocm@gmail.com

Un mail

Delivered-To: d.sergiocn@gmail.com
Received: by 10. [REDACTED] with SMTP id ao2csp15350181bc;
Mon, 11 Apr 2016 18:31:37 -0700 (PDT)
X-Received: by 10.28.30.79 with SMTP id e76mr20869055wme.27.1460395897818;
Mon, 11 Apr 2016 18:31:37 -0700 (PDT)
Return-Path: <sergioc@derechonntt.com>
Received: from [REDACTED]
by mx.google.com with ESMTP id v124s119484889wmg.0.2016.04.11.10.31.37
for <d.sergiocn@gmail.com>;
Mon, 11 Apr 2016 18:31:37 -0700 (PDT)
Received-SPF: pass (google.com: domain of sergioc@derechonntt.com designates 195. [REDACTED] as permitted sender) client-ip=195. [REDACTED];
Authentication-Results: mx.google.com;
dkim=pass header.i=@derechonntt.com;
spf=pass (google.com: domain of sergioc@derechonntt.com designates 195. [REDACTED] as permitted sender) smtp.mailfrom=sergioc@derechonntt.com
Received: from www.derechonntt.com (localhost [IPv6:::1])
by [REDACTED] (Postfix) with ESMTP id 6C07C59E1D88
for <d.sergiocn@gmail.com>; Mon, 11 Apr 2016 19:31:07 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=derechonntt.com;
s=mail; t=1460395867;
bh=LPO0hPie+kFzvxQWDPjG8eRkyoCKfPQ8SeabvklZOM=;
h=Date:From:To:Subject;
b=SfQAR79kgd8kseD7P/c4jrSRL4j7cR3M2qU3qH1sKiQEz1DPHTtVisE1xW4PFb8wy
cOwixHPLhftQn4PbY0mWKnERHDIjCt/xiWpVCIYPFhtrgZuOxXC0MQBUcveOXP0HH2
HxaX++64DIITPLQw/1CuTDEFAu37F1P4Z/rBB204=
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII;
format=flowed
Content-Transfer-Encoding: 7bit
Date: Mon, 11 Apr 2016 19:31:07 +0200
From: Sergio Carrasco Mayans <sergioc@derechonntt.com>
To: d.sergiocn@gmail.com
Subject: Mail
Organization: Derecho en Red
Message-ID: <2296ee490a237fe09fa33d171da0adff@www.derechonntt.com>
X-Sender: sergioc@derechonntt.com
User-Agent: Roundcube Webmail/1.1.0

Un mail

DEPRECATED

The author's user ID.

The author of the tweet. This embedded object can get out of sync.

IDs are roughly sorted & developers should treat them as opaque (<http://bit.ly/dCkppc>).

Consecutive duplicate tweets are rejected. 140 character max (<http://bit.ly/4ud3he>).

```
{ "id"=>12296272736,
  "text"=>
  "An early look at Annotations:
  http://groups.google.com/group/twitter-api-announce/browse_thread/thread/fa5da2608865453",
  "created_at"=>"Fri Apr 16 17:55:46 +0000 2010",
  "in_reply_to_user_id"=>nil,
  "in_reply_to_screen_name"=>nil,
  "in_reply_to_status_id"=>nil,
  "favorited"=>false,
  "truncated"=>false,
  "user"=>
  { "id"=>6253282,
    "screen_name"=>"twitterapi",
    "name"=>"Twitter API",
    "description"=>
    "The Real Twitter API. I tweet about API changes, service issues and
    happily answer questions about Twitter and our API. Don't get an answer? It's on my website.",
    "url"=>"http://apiwiki.twitter.com",
    "location"=>"San Francisco, CA",
    "profile_background_color"=>"cldfee",
    "profile_background_image_url"=>
    "http://a3.twimg.com/profile_background_images/59931895/twitterapi-background-new.png",
    "profile_background_tile"=>false,
    "profile_image_url"=>"http://a3.twimg.com/profile_images/689684365/api_normal.png",
    "profile_link_color"=>"0000ff",
    "profile_sidebar_border_color"=>"87bc44",
    "profile_sidebar_fill_color"=>"e0ff92",
```

Tweet's creation date.

The ID of an existing tweet that this tweet is in reply to. Won't be set unless the author of the referenced tweet is mentioned.

The screen name & user ID of replied to tweet author.

Truncated to 140 characters. Only possible from SMS.

The author's user name.

The author's biography.

The author's screen name.

The author's URL.

The author's "location". This is a free-form text field, and there are no guarantees on whether it can be geocoded.

Rendering information for the author. Colors are encoded in hex values (RGB).

The creation date for this account.

El testimonio de la víctima

El Tribunal Supremo establece que el testimonio de la víctima constituye por sí solo prueba bastante para enervar la presunción de inocencia siempre que concurren determinados requisitos: verosimilitud, persistencia en la incriminación y ausencia de móviles espurios como resentimiento o venganza.

Mientras en el caso del acusado puede callar, en todo o en parte, o mentir, porque se le reconoce tal derecho, en el caso de la víctima está sujeta a la obligación de decir verdad, so pena de cometer delito de falso testimonio.

Y eso hace que en derecho Penal, a diferencia de lo que ocurre en los demás campos del Derecho, ambos testimonios no tengan la misma naturaleza. Por tanto, cuando contamos con la declaración de la víctima no es que no haya prueba, es que ésta ya es una prueba en sí misma.

El testimonio de la víctima, además, cobra un especial valor cuando viene reforzado por otros indicios circunstanciales u otras pruebas que confirmen su versión.

Sería el caso de un parte médico que constatará unas lesiones compatibles con el relato de hechos de la víctima.

Todas las pruebas habrán de ser valoradas en su conjunto, aplicando el principio de libre valoración de la prueba que establece la ley de Enjuiciamiento Criminal.

El papel de los operadores de telecomunicaciones

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Artículo 1 Objeto de la Ley

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.
2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.
3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Varias sentencias han considerado la violencia de género como un delito grave:

Sentencia núm. 2290/2011 de 14 Oct. Del Tribunal Superior de Justicia de Castilla y León de Valladolid, Sala de lo Contencioso-administrativo, núm. De Rec. 284/2011.

Sentencia núm. 467/2014 de 30 Abr. Del Tribunal Superior de Justicia de Andalucía de Sevilla, Sala de lo Contencioso-administrativo, Sección 3ª, núm. De Rec. 123/2014.

Sentencia núm. 426/2016 de 30 Sep. Del Tribunal Superior de Justicia del País Vasco, Sala de lo Contencioso-administrativo, Sección 3ª, núm. De Rec. 113/2016.

Sentencia núm. 1330/2016 de 3 Oct. Del Tribunal Superior de Justicia de Castilla y León de Valladolid, Sala de lo Contencioso-Administrativo, núm. De Rec. 239/2016.

Sentencia núm. 3200/2016 de 19 Dic. Del Tribunal Superior de Justicia de Andalucía de Granada, Sala de lo Contencioso-administrativo, núm. De Rec. 436/2015.

EXTRACTO DE LAS SENTENCIAS:

*“Los delitos de violencia de género afectan a la seguridad pública. Destaca que **la protección del derecho de todos, en particular de las mujeres, a vivir a salvo de la violencia, tanto en el ámbito público como en el ámbito privado, es una cuestión de seguridad pública y, por tanto, responsabilidad del Estado.** Recuerda en este sentido que la normativa española ha configurado los delitos de violencia de género en el ámbito de la pareja como delitos de naturaleza pública, no privada, perseguibles de oficio. Concluye de este modo que **los delitos de la violencia de género afectan a la seguridad pública, en cuanto suponen una amenaza o un atentado grave a un interés fundamental de la sociedad, cual es el de proteger la dignidad e integridad física y moral de las personas que la integran, en este caso las mujeres vinculadas por matrimonio o relación análoga de afectividad**”.*

¿Y si la llamada se hace desde un número oculto?

El operador de telecomunicaciones está obligado a identificar y conservar el número de origen y de destino y a facilitarlo cuando lo pida un juez.

La llamada es anónima para el usuario pero no para el operador, que la puede rastrear sabiendo día, hora y número que ha recibido la llamada.

Derechos ARCO

Derecho de oposición

El derecho de oposición es uno de los derechos que la Ley Orgánica de Protección de Datos de carácter personal (LOPD) reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario

¿Y si me están espiando el móvil?

Hay señales externas que pueden ponernos sobre aviso de que algo extraño está ocurriendo, aunque sean tan solo indicios:

- **-La batería se consume con rapidez:** El 'spyware' o programa espía permanece activo, lo que provoca un acortamiento de la batería del teléfono.
- **-Sube el uso de datos móviles:** al enviar información desde el teléfono hasta los servidores de la aplicación, ésta necesita hacer uso de más capacidad de red, lo que eleva el consumo de datos.
- **-Temperatura elevada del dispositivo:** si nuestro teléfono nos avisa de que la CPU ha alcanzado una temperatura alta, una de las posibilidades es que sea debido a una aplicación espía.

Puede ser un virus y no un programa espía.

¿Qué hago si creo que espían mi teléfono?

a) Utilizar *antispyware*. La primera medida que podemos tomar es la instalación de alguna aplicación especializada que nos permitirá detectar la mayoría de programas espía instalados.

Se conocen como “antispyware”. Además de protección contra software espía, también nos aporta otras funciones de seguridad y optimización del teléfono, como antivirus completo y limpieza de archivos basura. Ejemplos CM Security o Anti Spy Mobile (ambas para Android)

b) Restaurar los valores originales. Si tras analizar con varias aplicaciones especializadas no aparece ninguna alerta de seguridad, podemos presumir que no tenemos el teléfono infectado.

No obstante, si tenemos sospechas de que nuestra información “tiene fugas”, podemos optar por restaurar el teléfono al estado de fábrica. Esta operación limpiará la memoria del dispositivo eliminando cualquier aplicación instalada que no sea original.

Eso sí, también borrará todos los archivos como fotos, vídeos, música o documentos descargados, por lo que deberemos realizar una copia de seguridad de los que queramos conservar.

Consejos prácticos

- Configurar las alertas para saber si otra persona accede a mis cuentas de Gmail, Facebook.
- Hacer copias de seguridad de disco duro del ordenador, de las conversaciones de Whatsapp, etc.
- Contraseñas seguras. Cambiarlas frecuentemente
- No dejar que terceros nos configuren el dispositivo sin estar presentes.

Otras opciones



A A+ A++



Quiénes Somos

Contacto

Q Busca

Movistar te ayuda a sacar el máximo provecho
de la tecnología y a usarla de manera segura y
responsable

Sostenibilidad ▼

Innovación ▼

Entretenimiento ▲

Identidad Digital ▼

Comportamiento ▼

Seguridad ▼

Otras opciones

¿Qué hacemos en STOP Violencia de Género Digital?

Asesoramiento Técnico Jurídico a víctimas de Violencia de Género Digital

Una vez que la víctima se ha puesto en contacto con nosotros:

1. Detectamos el tipo de delito al que está siendo sometida la víctima
2. Se analizan los dispositivos por los cuales está siendo la víctima atacada, en busca de evidencias o registros que puedan respaldar la acusación de la víctima
3. Procedemos a indicarles cuales son las medidas legales que pueda tomar contra el ciberatacante
4. Realizamos el informe pericial en el cual queda constancia las evidencias digitales encontradas en el terminal, todo ello siguiendo una cadena de custodia para salvaguardar las evidencias
5. En caso necesario se ratifica el informe en sala
6. Implantamos un software que nos ayuda a detectar posibles nuevos ataques
7. Y por último, le enseñamos a la víctima a protegerse ante posibles ciberacosadores

¡muchas gracias!

