

Anna Saludes Ferrer

LA SOMBRA DE INTERNET

TRABAJO DE FINAL DE GRADO

Dirigido por el Catedrático Gonzalo Quintero Olivares

Grado en Derecho



Tarragona,

2016

Resum

Els delictes evolucionen amb les persones, ja que cada vegada són més complexos i realitzats amb mitjans diversos. La presència de les TIC en la vida de les persones ha afavorit a que incrementin exponencialment els delictes informàtics, i sobretot la dificultat per determinar l'autor del delicte. És per això que el treball analitza amb profunditat la comissió dels delictes informàtics, i sobretot es centra amb els delictes de violació de la intimitat, i més concretament amb el sexting, que és un delicte que produeix un perjudici important en la vida personal, però la víctima prèviament ha permès l'entrada d'un tercer en la seva vida íntima, és per aquest motiu que el legislador estableix una pena ínfima en relació al dany causat. Si voleu descobrir més sobre tot el món dels delictes informàtics i el sexting, endinseu-vos en aquest treball...

Resumen

Los delitos evolucionan con las personas, porque cada vez son más complejos y realizados con medios diversos. La presencia de las TIC en la vida de las personas ha permitido que incrementen exponencialmente los delitos informáticos, y sobretodo ha dificultado determinar el autor del delito. Es por ese motivo que el trabajo analiza con profundidad la comisión de los delitos informáticos, y concretamente se centra en los delitos de violación de la intimidad, analizando con precisión el sexting, que es un delito que produce un perjuicio importante en la vida personal, pero la víctima previamente ha permitido la entrada de un tercero en su vida íntima, es por ese motivo que el legislador establece una pena ínfima en relación con el daño causado. Si queréis descubrir más sobre todo el mundo de los delitos informáticos y el sexting, adentraros en este trabajo...

Abstract

Crimes evolve with people, because they are becoming more complex and performed with various media. The presence of ICT in the lives of people allowed to increase exponentially cybercrime, and above all has made it difficult to determine the perpetrator. It is for this reason that this research work analyzes in depth the commission of cybercrime, and specifically focuses on the crimes of violation of privacy, accurately sexting, which is a crime that causes material injury in personal life, but the victim has previously allowed the entry of a third in his private life, is for this

reason that the legislature makes a negligible pity in relation to the damage caused. If you want to find out more about the whole world of cybercrime and sexting, step into this research paper...

Paraules clau / Palabras clave / Keywords

Delitos informáticos – Sexting – Derecho a la intimidad – Privacidad – Libertad sexual –
Cybercrime – Privacy – Amenazas – Adolescentes – Unidad de Investigación de personas

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer el apoyo de mi Tutor, el Sr. Gonzalo Quintero para ayudarme y facilitarme la búsqueda de información ya que al ser un tema muy novedoso me ha sido muy útil su experiencia y conocimientos de Derecho Penal. Por otro lado me gustaría agradecerle también la voluntad de ayudarme a mejorar y perfeccionar el trabajo.

En segundo lugar, me gustaría agradecer los consejos que he recibido por parte de Núria Torres y Maria Marquès, ya que aún y no siendo mis tutoras me han ayudado a estructurar mejor el trabajo y guiarme con toda predisposición.

También me gustaría agradecer el apoyo incansable de mi familia personalmente a mi padre, mi madre y mi hermana que en los momentos de debilidad de toda mi vida, y evidentemente en la carrera, me han aconsejado y animado a seguir para conseguir mis objetivos. Sin ellos no sería la persona que soy y no hubiera llegado donde he llegado.

Por último me gustaría agradecer a mi pareja, Joan, por apoyarme y animarme en todo sin excusa ni excepción. Sin él este trabajo, seguramente no se hubiera enfocado de la misma manera.

SUMARIO

ABREVIATURAS	9
INTRODUCCIÓN.....	11
CAPÍTULO I. REFERENCIA AL CONCEPTO DE DELITO INFORMÁTICO ...	13
1.1. Clasificación de delitos informáticos.....	14
1.1.1. Delitos económico-patrimoniales vinculados a la informática:	
ciberdelincuencia económica	14
1.1.2. Atentados por medios informáticos contra la intimidad y la privacidad:	
ciberdelincuencia intrusiva.....	15
1.1.3. Ataques por medios informáticos contra intereses supraindividuales:	
ciberespionaje y ciberterrorismo	16
CAPÍTULO II. ANÁLISIS DE LA EVOLUCIÓN DE LOS DELITOS	
INFORMÁTICOS	17
CAPÍTULO III. REGULACIÓN NACIONAL E INTERNACIONAL.....	23
CAPÍTULO IV. DIFICULTADES PARA DETERMINAR LA AUTORÍA, LA	
COMPETENCIA Y LA PENA DE LOS DELITOS INFORMÁTICOS	31
CAPÍTULO V. DELITOS CONTRA LA INTIMIDAD PERSONAL, EL HONOR Y	
A LA LIBERTAD SEXUAL POR MEDIOS INFORMÁTICOS.	37
5.1. Sexting	37
5.1.1. Sujetos del delito	46
CAPÍTULO VI. UNIDAD CENTRAL DE DELITOS INFORMÁTICOS DE LOS	
MOSSOS D'ESQUADRA	49
CAPÍTULO VII. ANÁLISIS DE UN CASO PRÁCTICO	57
CAPÍTULO VIII. CONCLUSIONES	61
BIBLIOGRAFIA	65
LEGISLACIÓN.....	69
JURISPRUDÈNCIA.....	71
WEBGRAFIA	73

ABREVIATURAS

Art. —————> Artículo

CP. —————> Código Penal

CE. —————> Constitución Española

Dir. —————> Directiva

Ibid. —————> Ibidem

L. —————> Ley

LO. —————> Ley Orgánica

LSSI —————> Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico

STS —————> Sentencia del Tribunal Supremo

SAP —————> Sentencia de la Audiencia Provincial

TIC —————> Tecnologías de la Información y Comunicación

INTRODUCCIÓN

El mundo de la informática actualmente ha permitido que la privacidad de las personas cada vez sea más poco respetada. Todas las redes sociales permiten que las personas publiquen su intimidad por todo el mundo sin poder predecir los perjuicios que este hecho puede producir.

A lo largo del siglo XXI se ha producido un incremento, generalizado y con una velocidad frenética, de la introducción de las nuevas tecnologías a la vida de las personas, produciéndose así una idea de vida incomprensible si no es con las nuevas tecnologías al alcance de todas las personas.

Es por esta razón que me he decantado por el estudio de las nuevas tecnologías en el ámbito del derecho penal. Considero que ser conocedor de estas modalidades delictivas ha de ser fundamental para entender hacia donde va la sociedad. Sociológicamente estos delitos tienen una enorme proyección de futuro, básicamente por tres razones muy claras, la primera, crecen desmesuradamente año a año este punto se desarrollará en el trabajo posteriormente, y la segunda, sus autores en la mayor parte de los casos son personas jóvenes que tienen altos conocimientos informáticos para imposibilitar su persecución por parte de la policía, y la tercera, que el nivel de protección de la vida privada cada vez está más obsoleto, actualmente la vida de las personas es pública en las redes sociales.

También se analiza si el legislador tiene que avanzar en la realización de normas que regulen los delitos informáticos, ya que la evolución de este tipo de delitos es cada vez más frecuente y los medios que se utilizan para cometerlos se perfeccionan, e incluso para borrar los rastros del autor del delito, para que cada vez sea más difícil poder ser castigados.

Por otra parte, yo me he querido centrar en un tipo específico de delitos electrónicos, en concreto al sexting uno de los tipos que afectan al ámbito de la intimidad y al propio honor de la víctima. Estos delitos producen un grave perjuicio para la víctima y su entorno, ya que la publicación de fotografías y aspectos íntimos de

la vida de la persona, produce una vulneración de su honor llegando incluso a una decadencia de la propia persona. Esta elección no es en vano, sino que una experiencia propia me ha permitido conocer y sufrir en primera persona el perjuicio que produce este tipo de delitos informático.

Para la realización de este trabajo he analizado los aspectos más generales hasta llegar a un análisis concreto de uno de los casos que pueden producirse a través de medios informáticos, por eso el trabajo se inicia con una breve referencia a qué se entiende por delito informático y conocer sus tres clasificaciones más comunes.

Posteriormente se analiza el crecimiento de la comisión de estos delitos, y en concreto los motivos que influyen en este crecimiento. Para poder entender como actúa el legislador ante tal crecimiento se analiza el conjunto de regulaciones a nivel internacional y estatal. Seguidamente, en el trabajo hay un apartado que analiza la problemática procesal para penar a las personas que cometen este tipo de delitos, ya que es habitual no poder determinar la competencia jurisdiccional o incluso el autor del delito.

Una vez analizados los delitos informáticos en general, el trabajo se centra en el estudio concreto del sexting, un tipo de delitos contra la intimidad personal que es cada vez más frecuente que se produzca, y la influencia que tiene entre los jóvenes. Sobre la base de las consideraciones era oportuno incluir en el trabajo una referencia al Departamento Central de Delitos Informáticos de los Mossos d'Esquadra, ya que es el departamento que se encarga de la investigación de estos delitos y para conocer más sobre su trabajo se ha realizado una entrevista con el responsable de la Unidad de Investigación de Personas, el inspector Jordi Domenech.

El trabajo finaliza con el estudio de forma práctica un caso habitual, y la determinación de la pena que tendría un delito de este tipo en el sistema normativo español y sus conclusiones respectivas.

CAPÍTULO I. REFERENCIA AL CONCEPTO DE DELITO INFORMÁTICO

Con el uso emergente de la tecnología informática, los delitos informáticos se han convertido en un importante reto mundial, al que hay que poner serias medidas de control y seguridad.

Partiendo de la afirmación realizada por QUINTERO cuando refiere¹ que "internet no es una simple progresión en la evolución tecnológica, sino un cambio revolucionario en los modelos de las relaciones sociales que sirve a la fluidez de los intercambios comerciales y de todo tipo", que trata de entender que se ha iniciado una revolución social partiendo de un hecho transformador y modificador de la vida en sociedad, que ha permitido al delincuente disponer de nuevas formas de actuación e incluso crear tipos delictivos ausentes años atrás.

En la dogmática penal actual se incluye en el concepto de delito informático tanto el delito tradicional cometido a través de ordenador, o Internet, como el propiamente tal, delito contra la informática, es decir, atacar los datos o sistemas informáticos o las vías telemáticas de comunicación². Por lo tanto tenemos dos ideas que se agrupan en un mismo concepto el propio delito a las redes informáticas y de Internet, y los delitos que se cometen a través y mediante Internet o un ordenador.

A continuación, algunas de las definiciones más reconocidas de lo que se entiende por delitos informáticos³:

- a) Para Ulrich Sieber los delitos informáticos, "*comprenden todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente*".
- b) La Organización para la Cooperación Económica y el Desarrollo (OCED) define los delitos informáticos como "*Cualquier conducta ilegal, no ética, o*

¹ Gonzalo Quintero Olivares, "Internet y derecho penal: imputación de los delitos y determinación de la competencia," *La ley penal: revista de derecho penal, procesal y penitenciario* (Wolters Kluwer, 2007), <https://dialnet.unirioja.es/servlet/articulo?codigo=2259130>.

² Eloy Velasco Núñez, *Delitos Cometidos a Través de Internet: Cuestiones Procesales* (Las Rozas (Madrid) : La Ley, 2010), http://cataleg.urv.cat/record=b1406593~S13*cat.

³ Emilio; Cisternas Hernández, "Análisis Y Proyección de Los Delitos Informáticos En Chile," *Universidad de Talca* 53, no. 9 (2013): 72, doi:10.1017/CBO9781107415324.004.

no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos”.

- c) El Departamento de Justicia Norteamericano entiende por delito informático, *“Cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación o persecución”.*

1.1. Clasificación de delitos informáticos

Dentro de este concepto tan amplio de delito cibernético, se podría establecer una tipología concreta de delitos informáticos:

1.1.1. Delitos económico-patrimoniales vinculados a la informática: ciberdelincuencia económica

Se trata de ataques al bien jurídico patrimonial ajeno, siempre y cuando se realicen a través de un sistema informático. Es importante destacar que tiene que haber intencionalidad de consumir apoderamientos o algún tipo de beneficio económico, y que este apoderamiento sea evaluable al patrimonio del tercero que este caso sería la víctima⁴. Por ese motivo es importante entender que la intencionalidad del sujeto activo debe ser cierta.

Es este tipo de delito informático el que más se denuncian en la autoridad, concretamente cerca del 70% del total de delitos cibernéticos. En el Código Penal, actual se prevén diversos tipos de delitos económico-patrimoniales vinculados a la informática:

- Robo inutilizando sistemas de guardia tipográfica (artículo 238.5 CP).
- Estafa informática, en su doble modalidad (artículo 248.2 CP).
- Defraudación de telecomunicaciones informáticas (artículo 255 CP).
- Uso no autorizado de terminales informáticos causando un perjuicio económico (artículo 256).

⁴ Velasco Núñez, *Delitos Cometidos a Través de Internet : Cuestiones Procesales*.

- Virus o daños informáticos, cuando se produce sobre datos (artículo 264.2 CP). Cuando los daños persiguen algo más que un ataque a los datos, nos encontraríamos frente a un sabotaje informático penado a través del delito de estragos (artículo 346 CP).
- Contra la propiedad intelectual informática, en cualquier de sus modalidades creativas reguladas (artículo 270.3 CP).
- Contra la propiedad industrial informática, en cualquiera de sus modalidades (artículos 273 – 275 CP).
- Publicidad engañosa (artículo 283 CP).
- Manipulación en aparatos en perjuicio del consumidor (artículo 286 CP).

1.1.2. Atentados por medios informáticos contra la intimidad y la privacidad: ciberdelincuencia intrusiva

Se trata de los ataques al bien jurídico de la privacidad, eso engloba a la intimidad y abarca todas las modalidades previstas en el artículo 18 de la CE, como es el derecho al honor, a la intimidad personal y familiar, el derecho a la propia imagen y el secreto de las comunicaciones. Concretamente en el artículo 18, establece que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, se desprende de este artículo la protección que el legislador debe conseguir con el establecimiento de medidas coercitivas y de protección para evitar la vulneración de estos derechos.

Suponen el 25% aproximado de los delitos que se denuncian se encuentran tipificados en el Código Penal actualmente:

- Amenazas y coacciones informáticas (artículo 169 y 172 CP)
- Distribución de material pornográfico y pornografía infantil (artículo 186 – 189 CP)
- Descubrimiento y revelación de secretos (artículo 197 - 200 CP). Este es el delito por excelencia de esta tipología de delitos informáticos.
- Injurias y calumnias informáticas

1.1.3. Ataques por medios informáticos contra intereses supraindividuales: ciberespionaje y ciberterrorismo

Estos delitos consisten en los ataques más graves, ya que afectan indiscriminadamente a intereses generales de la población, es decir afecta a una gran parte de individuos produciendo un perjuicio, con la intención de crear pánico y terror, para subvertir el sistema político o de convivencia generalmente aceptado.

Este tipo de delitos es el menos realizado ya que es necesario una organización terrorista o una agrupación organizada de personas. Aún así su realización al afectar a una gran masa de persona provoca mucha inquietud.

Algunas de las modalidades en nuestro Código Penal actual son “Ley Orgánica 10/1995, de 23 de Noviembre, Del Código Penal. TÍTULO XIII. Delitos Contra El Patrimonio Y Contra El Orden Socioeconómico.” n.d.:

- Usurpación de funciones públicas mediante correo electrónico (artículo 420 CP)
- Descubrimiento y revelación de secretos relativo a la defensa nacional (artículo 598 y 603 CP)

CAPÍTULO II. ANÁLISIS DE LA EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS

En la actualidad la evolución de los delitos informáticos es muy importante, se han producido diversos estudios que lo demuestran. Los adelantos en la tecnología de las comunicaciones han determinado que surgieran nuevas oportunidades para la comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en la Internet, y esas oportunidades han sido explotadas por los grupos delictivos organizados. La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia⁵.

En definitiva, la rapidez, el anonimato, la comodidad y la amplitud de alcance que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas, tanto tradicionales aprovechando los nuevos medios, como otras nuevas nacidas dentro de este ámbito. La apertura de nuevos mercados y las nuevas TIC, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo⁶.

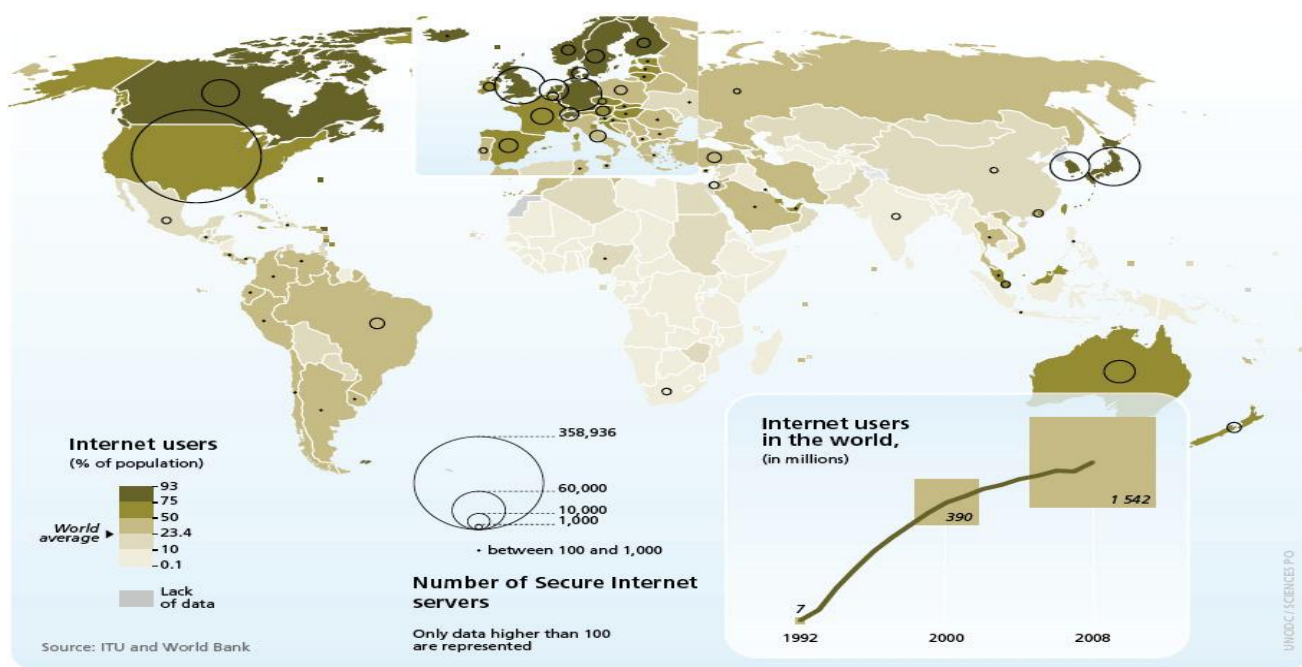
Las materializaciones más populares de la sociedad de la información, y de las TIC, las forman la triada que componen el ordenador personal, Internet y la telefonía móvil. El crecimiento en el número de ordenadores ha sido vertiginoso y si en 1945 apareció el primer ordenador, a finales de 2012 se habían ya superado los 2.000 millones de ordenadores. El año de nacimiento de Internet para la sociedad, finales de 1995, contaba ya con unos 16 millones de usuarios. Apenas quince años después, a finales de 2010, ya existían en torno a 2.000 millones de usuarios. En la actualidad se estima que, alrededor de una tercera parte de la población del planeta (7.000 millones) accede a Internet. Y en los países más desarrollados, los que pueden ser denominados de manera plena como

⁵ Marta María Aguilar Cárceles, "Cybercrime and Cybervictimization in Europe: Institutions Involved in Cybercrime Prevention in the United Kingdom," *Revista Criminalidad* 57, no. 1: 121–35, accessed March 5, 2016, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082015000100009&lng=en&nrm=iso&tlng=es.

⁶ Juan María; Martínez Otero, "La Difusión de Sexting Sin Consentimiento Del Protagonista: Un Análisis Jurídico," no. 12 (2013): 1–16.

sociedades de la información y del conocimiento, entre los jóvenes (la cohorte de 16 a 29 años) la tasa de uso de Internet supera el 90% de este colectivo social⁷

Por todo esto que la evolución en torno a todos los delitos por medios tecnológicos es importante, a continuación en la imagen se puede ver la utilización de las TIC en el mundo, como podemos observar la incidencia de las nuevas tecnologías se centra en Estados Unidos, Europa, Canadá Japón y Australia. Por lo tanto se desprende la idea que en estos países será donde la incidencia de los delitos informáticos será más elevada ya que el uso de las nuevas tecnologías influye mucho en el desarrollo de estos delitos. Otro dato importante que se desprende de este estudio son la cantidad de servidores de seguridad, ya que en Europa aunque hay un elevado número de internautas existen pocos servidores de seguridad, a diferencia de Estados Unidos que es donde se contabilizan el mayor número de servidores, comprobamos pues que la seguridad en Estados Unidos es más elevada respecto Europa o incluso Canadá.



- Marco Gerke, “The Global Challenge,,” *Population Reports. Series M. Special Topics*, no. 15 (2000): 1–2.

⁷ Cristóbal (Dir.) Torres Alberó, José Manuel Robles, and Stefano De Marco, “El Ciberacoso Como Forma de Ejercer La Violencia de Género En La Juventud: Un Riesgo En La Sociedad de La Información Y Del Conocimiento,” 2013, 165, doi:NIPO: 680-13-092-1.

Una vez analizado el número de internautas, cabe destacar que podemos comprobar que en los países desarrollados hay una mayor probabilidad que se cometan delitos informáticos que en los países subdesarrollados ya que evidentemente al no estar presente las nuevas tecnologías en la vida común de las personas, menos medios hay para cometerlos.

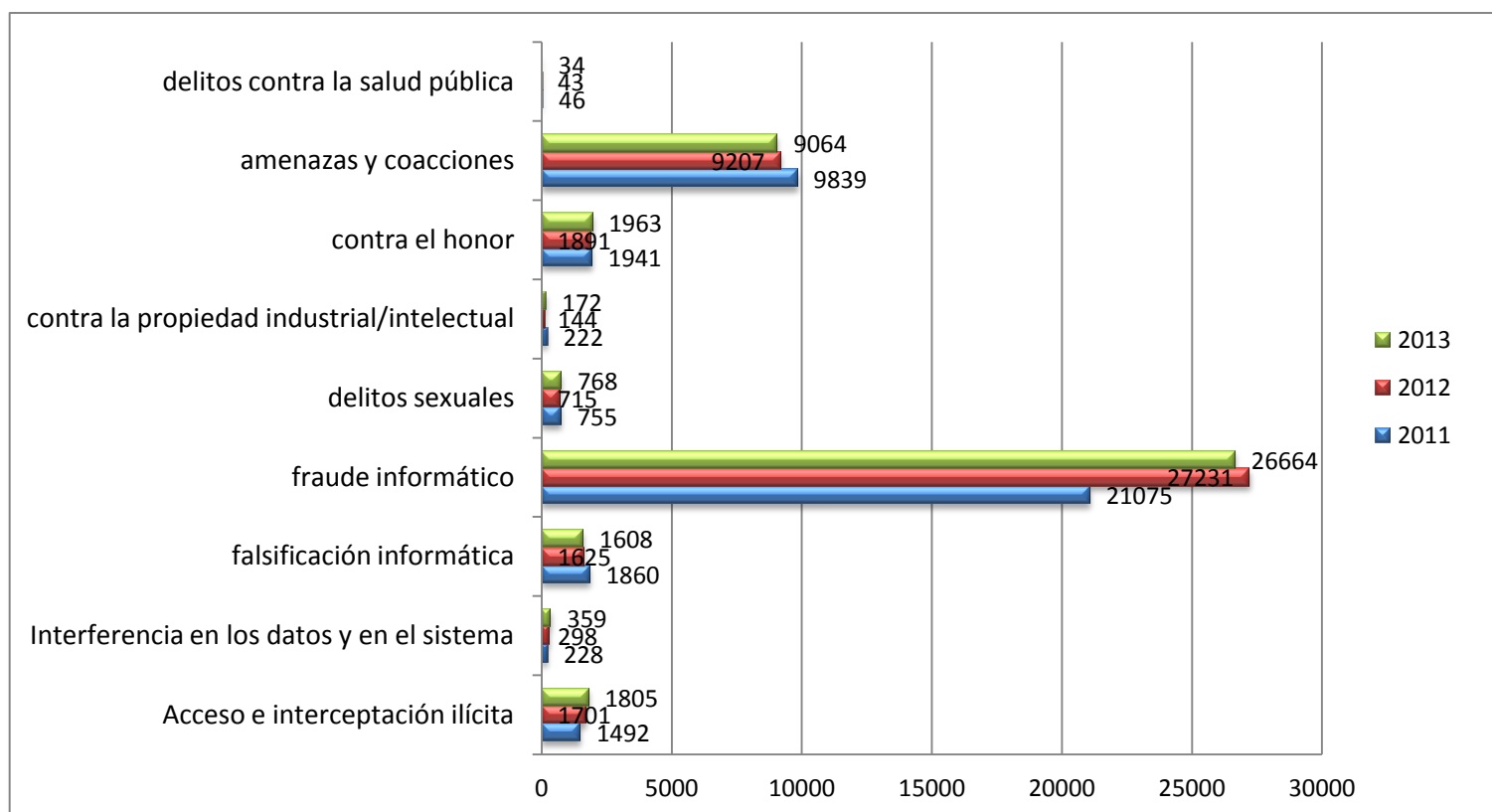
Este aumento se debe por un lado, a la propia evolución y desarrollo de nuevas tecnologías, que cómo ya se ha comentado, ha hecho posible la aparición de nuevas formas de delinquir a través de internet, cada vez más sofisticadas y efectivas. Y de por otro lado, cada vez son más las personas, instituciones y empresas que utilizan las nuevas tecnologías e internet en ámbitos de la vida y los negocios, lo cual genera un mayor número de oportunidades para que los cibercriminales puedan actuar. Se entiende por tanto que el aumento de la utilización de las tecnologías lleva consigo una creciente utilización de ella por la comisión de delitos mediante internet o a internet.

El sujeto activo en el delito ha pasado de ser un solo sujeto experto en internet con alta disponibilidad de tiempo para cometer delitos informáticos, a un conjunto de sujetos organizados que su afán delictivo es apoderarse de dinero ajeno a gran escala tal y como remarca el autor VELASCO NÚÑEZ⁸. En los últimos años los delitos informáticos han crecido desmesuradamente año a año, en el siguiente gráfico podemos comprobar cómo entre los años 2011 a 2013 ha aumentado todo tipo de delitos informáticos, aunque el fraude informático es el que más crece concretamente un 26,51% (5.589 casos más al año). Estos datos deberían producir preocupación al legislador ya que la forma de producir un delito está cambiando, ergo tendrían que actualizar las penas y la tipología jurídica de los delitos informáticos para evitar así la impunidad delictiva⁹.

Analizándolo se comprueba a simple vista que los delitos de fraude informático són los más realizados con diferencia y su crecimiento ha sido bastante importante en el 2012, y aunque se ha reducido mínimamente en el año 2013 sigue siendo el delito más cometido.

⁸ Velasco Núñez, *Delitos Cometidos a Través de Internet : Cuestiones Procesales*.

⁹ Ministerio del Interior (gabinete de Coordinación y Estudios), “Anuario Estadístico de Ministerio Interior,” BOE 53, no. 9 (2013): 15, doi:10.1017/CBO9781107415324.004.



- Datos del Anuario Estadístico del Ministerio del Interior de España¹⁰

También es fácil comprobar, que el delito de amenazas y coacciones a través de internet es el segundo más cometido, esto se deduce ya que muchos de los delitos informáticos no se cometen si antes no se ha producido una amenaza para conseguir un objetivo, por ejemplo, que el delito contra el honor y la intimidad que analizaremos en profundidad no se comete sin antes no realizar una amenaza con un objetivo, ya sea dinerario o de algún hecho concreto. Esto es así, ya que es habitual en este tipo de delitos que se produzca el concurso delictivo.

Esta creciente evolución ha propiciado que el legislador intente regular las conductas, ya que si estas no son codificadas no podrán ser punibles. La consecuencia principal de este análisis es que la evolución de estos delitos es imparable, ya que las tecnologías cada vez están más presentes en todas las esferas de la vida de la persona, facilitando así la comisión de actos ilícitos mediante estas. En conclusión pues, los delitos informáticos no sólo aumentan en cantidad, también lo hacen en variedad debido al progreso tecnológico y al creciente uso de internet por los ciudadanos, y los

¹⁰ Ibid.

legisladores han tenido que hacer frente a esta circunstancia aportando respuesta ágiles que faciliten la protección de los usuarios, tanto empresas como particulares.

Ante esta situación, la legislación española ha debido responder a lo largo de los últimos años con el fin de proteger a los ciudadanos frente a estas constantes amenazas. Esta respuesta llega de dos formas íntimamente ligadas, por una parte, la reforma legislativa que se va realizando cada vez se incluyen más modalidades de delitos informáticos. Por otra parte, dotas a los agentes indicados de los instrumentos y herramientas necesarias que faciliten la investigación y esclarecimiento de los hechos.

Aún así, la necesidad de establecer normas concretas a los actos delictivos concretos es evidente, ya que aún siguen siendo muchos los delitos que no están tipificados, debido a la lentitud del legislador en adaptar la normativa a las conductas de las personas. Es por eso que es necesario incrementar la prevención sobretudo en niños y adolescentes, ya que son las personas más vulnerables y las que crecen con una mayor influencia de las TIC.

Este aumento se traduce en los siguientes datos plasmados en la Instrucción 2/2011 de la Fiscalía General¹¹, sobre el Fiscal de Sala de Criminalidad Informática y las secciones de criminalidad informática de las Fiscalías relativa al año 2014, arrojan un total de 20.534 delitos informáticos conocidos por el Ministerio Fiscal. Esta suma total representa un aumento del 71,21% respecto al año inmediatamente anterior, 2013, en que la cifra se situó en los 11.990 delitos, y un incremento de más del 210% en relación a los 6.532 delitos informáticos identificados en 2011. Dicho en otras palabras, en los cuatro años que abarcan el período de 2011 a 2014, el número de delitos informáticos ha pasado de 6.532 a 20.534, casi se ha cuadruplicado.

Estas cifras aún podrían esconder un mayor número de delitos vinculados a las TIC pues, este tipo de delincuencia presenta una enorme transversalidad y sus comportamientos ilegales pueden ser de diferente naturaleza y, por tanto, encuadrarse en tipos penales muy diferentes. La consecuencia es que en ocasiones, un delito

¹¹ Fiscalía, “Instrucción 2/2011 Sobre El Fiscal de La Sala de CRIMINALIDAD INFORMÁTICA Y LAS SECCIONES DE CRIMINALIDAD INFORMÁTICA DE LAS FISCALÍAS,” 2011, 2074–94.

informático puede quedar oculto porque no se establece dentro de la jurisdicción penal sino de la jurisdicción civil tal y como ocurría con el sexting antes de la última Reforma Penal. Si unimos esto con el hecho que muchas personas aún no denuncian este tipo de acciones delictivas, el resultado es que las cifras reales serían incluso mayores que las expuestas.

CAPÍTULO III. REGULACIÓN NACIONAL E INTERNACIONAL

Cada vez es más frecuente la realización de delitos que vulneran la intimidad mediante las TIC, por eso el legislador ha regulado las conductas más realizadas y las ha tipificado como delito, y en consecuencia estableciéndoles una pena. La percepción social de la peligrosidad de estas actuaciones y las evidentes dificultades para su descubrimiento y persecución, así como para la identificación de las personas responsables de estos comportamientos, han determinado una decidida actuación del legislador.

Esta regulación se ha ido promoviendo principalmente a nivel internacional con convenios multilaterales, para forzar la regulación estatal de los diferentes estados. El ejemplo más claro para intentar regular la problemática de los delitos informáticos es el Convenio de Budapest, ratificado por España el 1 de octubre de 2010 por el que se establecen las unidades de medida. Este convenio establece una clasificación de las distintas modalidades de delitos informáticos en los que se engloba el fraude informático, la pornografía infantil o delitos contra la propiedad intelectual entre otros. Pero esto no es realmente relevante, lo que realmente importante del Convenio Internacional, es el articulado relativo a las medidas procesales para inculpar a los autores de los delitos informáticos, y el establecimiento de medidas de cooperación internacional en figuras como la extradición y la asistencia mutua para investigar estos delitos¹². El problema principal de los convenios internacionales es la falta de concienciación de los gobiernos estatales para ratificarlos, como en este caso que lo han ratificado muy pocos estados.

Por otra parte el Consejo de Europa, ha realizado distintas recomendaciones para evitar el perjuicio que pueden llegar a tener los delitos a través de las TIC, entre las que destacamos la Recomendación (2001) 18, relativa a la autorregulación de los contenidos cibernéticos (autorregulación y protección de usuarios contra los contenidos ilegales o dañinos de los nuevos servicios de comunicación e información), Recomendación CM/Rec (2008) 6, sobre medidas para promover el respeto a la libertad de expresión e información en atención a los filtros de Internet, Recomendación CM/Rec (2009) 5,

¹² María Marta González Tascón, "El Nuevo Delito de Acceso a Niños Con Fines Sexuales a Través de Las TIC," *Estudios Penales Y Criminológicos XXXI*, no. 31 (2011): 207–58.

sobre medidas para proteger a los niños de contenidos y comportamientos dañinos y para promover su participación activa en el nuevo escenario de la información y las comunicaciones¹³.

En la misma línea de protección a los adolescentes y niños, se ha ido regulando la materia en Europa, y se ha promovido una reforma en los Estados Miembros de su regulación penal, ya que la Directiva 2011/93/UE de 13 de diciembre de 2011¹⁴, que deroga la Decisión Marco 2004/68, establece que la fijación de unas normas mínimas respecto a la definición de las infracciones penales y de las sanciones incluyendo también medidas para reforzar la prevención de estos delitos y la protección de sus víctimas. Esta Directiva es la que ha forzado a la realización de cambios en el Código Penal Español, como la introducción de la práctica de sexting¹⁵. Otra directiva es la 2000/31/CEE creando un sistema de responsabilidad penal a nivel Europeo, esta ha sido traspuesta al Estado Español mediante la Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico. Esta ley sirve para determinar la autoría en casos de delitos relacionados con la informática es por eso que se analizará en el siguiente Capítulo.

Desde el punto de vista estatal, en España desde la aprobación del Código Penal en el año 1995 ha sido objeto de importantes reformas en materia libertad sexual y contra la intimidad. La nueva reforma del Código Penal ha regulado las distintas modalidades de delitos contra la intimidad mediante la utilización de las TIC, como ya hemos apuntado debido a la aprobación de directivas europeas. Concretamente la Ley Orgánica 1/2015, de 30 de marzo, ha añadido el sexting mediante el artículo 183.1 ter i 197.7 del Código Penal, aunque según la doctrina esta regulación se ha realizado con defectos técnicos de comprensión, y perjudica la claridad sistemática que se establecía en el Código¹⁶. Los dos artículos han añadido la práctica ilícita del sexting, y han establecido la pena privativa de libertad como pena, aunque el artículo 183.1 ter se refiere a la publicación de archivos con carácter sexual de menores, dicho de otra manera a la

¹³ Ibid.

¹⁴ Directiva Ue, D E L Parlamento, and Europeo Y Del, “Directiva 2011/93/UE, Relativa a La Lucha Contra Abusos Sexuales Y La Explotación Infantil,” 2011, 1–14.

¹⁵ Gonzalo Quintero Olivares, *Comentario a La Reforma Penal de 2015* (Cizur Menor, Navarra : Thomson Reuters Aranzadi, 2015), http://cataleg.urv.cat/record=b1496194~S13*cat.

¹⁶ Ibid.

pornografía infantil, en cambio el artículo 197 está referido a la revelación de secretos que sería de aplicación por los casos que sea la víctima mayor de 16 años¹⁷.

Profundizando en el estudio de los dos artículos, por una parte el artículo 183 ter primer apartado se está refiriendo a una práctica conocida en el ámbito jurídico-penal como grooming. Esta práctica consiste en el acercamiento por parte de un adulto a menores con una finalidad sexual a base de la realización por aquel de ciertos comportamientos dirigidos precisamente a prepararle para que ceda ante sus pretensiones sexuales, siendo parte fundamental de ese proceso el hecho de ganarse la confianza del menor, ya que sin confianza el menor no accede a la pretensión sexual¹⁸. Este fenómeno ha cobrado en los últimos años una nueva forma de manifestarse, tal y como nos hemos referido al inicio, como consecuencia de evolución en la utilización de instrumentos de los que se sirve el sujeto para llevarlo a cabo, en otras palabras, las nuevas tecnologías de la información y de la comunicación, particularmente Internet (*online child grooming*); que, como es sabido, representan para muchos niños y jóvenes un componente significativo de su vida social¹⁹. Cabe destacar que cada vez es más temprana la edad en la que los menores se introducen en las redes sociales y en el mundo de la tecnología por eso incrementan los casos de este tipo de delito. Lo que destaca de la nueva reforma penal, es el aumento de la edad en la que se establecía este delito, la edad antes prevista era la de trece años y ahora asciende a dieciséis. La finalidad del legislador ha sido la de aumentar las condenas por este delito ya que la edad mayoritariamente que se utilizan las TIC es entre 13 y 16 años.

Por otra parte el artículo 183 ter segunda parte supone la introducción de ex novo, la conducta del sexting. Esta conducta es la que se analizará en profundidad tanto de forma práctica como teórica debido a su novedosa incorporación en la sociedad. Para poder paliar los problemas derivados tanto de esta práctica como del hecho de que el anonimato en internet permite una capacidad de engaño a las personas, y aún más a los menores, el legislador lo regula mediante la Reforma de 2015.

¹⁷ José L. González Cussac, Ángela Matallín Evangelio, and Elena Górriz Royo, *Comentarios a La Reforma Del Código Penal de 2015* (Valencia: Tirant lo Blanc, 2015), http://cataleg.urv.cat/record=b1496059~S13*cat.

¹⁸ Tascón, "El Nuevo Delito de Acceso a Niños Con Fines Sexuales a Través de Las TIC."

¹⁹ Ibid.

En este apartado el legislador estructura el delito en tres apartados concretos:

- Contacto con un menor de 16 años, a través de las TIC.
- Realización de actos materialmente tendentes a embaucarle
- Finalidad principal, es que el menor le envíe o muestre imágenes de pornografía de menores.

Esta estructura produce una serie de problemas a la hora de su interpretación, sobretudo el verbo embaucar. Ya que se supone que son las conductas que suponen un engaño en el que el menor podría caer por su ingenuidad en materia sexual, dicho en otras palabras, no basta con el engaño sino que debe probarse que existen actos dirigidos a un aprovechamiento de la inexperiencia sexual del menor y un riesgo serio para el bien jurídicamente protegido, como es la esfera sexual del menor y garantizar su bienestar psíquico, desarrollo y proceso de formación sexual²⁰. Hay doctrina que entiende que no se aplicará este precepto si es el propio menor el que *motu proprio* envía los archivos de contenido sexual, aunque desde otro punto de vista es evidente que el hecho que embauchen a una persona hace que este realice acciones que no son voluntarias, criticando pues la postura de esta parte de doctrina se tendría que incluir perfectamente el envío al adulto de forma “voluntaria” de estos archivos, aunque por otra parte se puede entender ya que se regula y tipifica esta conducta voluntaria, en el artículo que a continuación se estudia.

Analizando el artículo 197.7 CP, vemos que es la introducción por parte del legislador, para dar respuesta a un problema que se ha venido produciendo, y agravando con el paso del tiempo, debido a la generalización del uso de las nuevas tecnologías. Este artículo recoge la conducta de divulgación de imágenes o grabaciones de una persona con contenidos sexuales que ha obtenido con su consentimiento pero sin contar con su autorización. Anteriormente a la Reforma de 2015, no se daba respuesta a este grave ataque a la intimidad, sino que se preveían los supuestos en los que la captación de las imágenes se hubiera realizado también de forma ilícita²¹. En la jurisprudencia cuando se planteaban este tipo de conductas que no estaban aún tipificadas en el

²⁰ González Cussac, Matallín Evangelio, and Górriz Royo, *Comentarios a La Reforma Del Código Penal de 2015*.

²¹ Ignacio Comes Raga, “La protección penal de la intimidad a través de la difusión in consentida del sexting ajeno,” *La ley penal: revista de derecho penal, procesal y penitenciario* (Wolters Kluwer, 2013), <https://dialnet.unirioja.es/servlet/articulo?codigo=4654389&info=resumen&idioma=SPA>.

Código, se remitía a la jurisdicción civil en base a la regulación establecida en la Ley Orgánica de 1/82 de 5 de mayo de protección civil del derecho al honor y a la intimidad personal y familiar, y a la propia imagen, tal y como se establece en la siguiente sentencia (SAP de Huelva, de 15 de febrero de 2002; JUR 2002, 115257):

La tutela penal de la intimidad personal recogida en el alegado art. 197, tiene por finalidad por un lado, impedir la difusión y revelación de datos perteneciente a la vida privada, a la esfera estrictamente personal, pero no cuando el conocimiento se ha obtenido por vía legítima. El art. 18 de la Constitución Española protege el derecho a la intimidad, pero no toda conducta que vulnere este derecho fundamental es, sin más, punible sino que el derecho penal como ultima ratio, se limita la tutela frente a acciones en las que se emplean medios insidiosos, así el art. 197,10 exige el empleo de artificios técnicos para la captación de imagen, y el consentimiento del titular en estos casos constituye siempre causa de atipicidad de la conducta. Y en este caso las imágenes reflejadas en la fotografías demuestran que fueron realizadas con consentimiento de las personas que aparecen en las misma. El origen ilícito de las imágenes es presupuesto para la aplicación de los tipos contenidos en los párrafos 2, 3 y 5 del art. 197, por el que se mantiene la acusación. No basta la divulgación aislada, ni su finalidad de dañar el honor de las personas. La exigencia de este origen ilícito en la obtención de las imágenes impide sancionar la conducta penalmente, con independencia de que al margen de esta tutela penal que se insta, el derecho a la propia imagen de la perjudicada pueda ser protección civilmente en el marco de la L.O.1/82 de 5 de mayo. El recurso debe ser desestimado y confirmada íntegramente la sentencia de instancia. Vistos los artículos y demás de general y pertinente aplicación

En cualquier caso, era una solución inadecuada puesto que, antes solo se consideraba que se vulneraba el derecho al honor, y es evidente que el derecho a la intimidad resulta gravemente dañado. Por eso el legislador ha considerado que se tiene que distinguir el consentimiento de la realización de una grabación o foto de uso privado de dos personas, y el consentimiento de la difusión estos archivos, ya que hay una importante distinción en la protección de la intimidad entre uno y otro.

Uno de los casos que ha provocado que el legislador en la nueva Reforma penal incluyera este tipo delictivo es el famoso Caso del Yébenes. Este fue producido en el año 2012, cuando una Concejala del Ayuntamiento del Yébenes envió vídeos con contenido sexual a un futbolista y este por error fue remitido al Alcalde, y este lo difundió por las redes sociales. Este procedimiento se ha tenido que suspender ya que la juez María del Carmen Neira considera que tal y como estaba redactado el antiguo artículo 197 CP no se podía inculpar por violación de la intimidad ya que la difusión del vídeo se hace de forma consentida cuando se produce el Sexting. Es por eso que la juez se planteaba la posibilidad de ser inculcados, los imputados por un delito de injurias²². Este fue uno de los litigios más famosos de estos tipos delictivos aunque evidentemente no el único ya que cada vez con más frecuencia las nuevas tecnologías permiten la comisión de este tipo delictivo.

Actualmente el TC, ha venido insistiendo en la evolución del concepto de intimidad personal, ya que en un primer momento se entendía como el derecho del titular a exigir la no injerencia de terceros en la esfera privada, entendiéndola como un derecho garantista o de defensa. Una segunda interpretación que realizó era a partir de la STC 134/1999 de 15 de julio, la intimidad se entendía pues como un bien jurídico que se relaciona con la libertad de acción del sujeto, con las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público. Por lo tanto vemos como en relación al nuevo artículo 197.7, considera que intenta proteger el derecho fundamental a la intimidad personal garantizando el artículo 18.1 de la CE, entendiendo la finalidad del legislador de proteger el ámbito propio y reservado de las personas.

Para poder alegar esta vulneración es necesario constatar la cesión i difusión de las fotografías, produciendo así un menoscabo a la intimidad de la persona. La regulación que se hace en el Código Penal del sexting en el caso que la víctima sea mayor de una dieciséis años de edad, es insuficiente la pena que se impone, ya que el legislador entiende que como se ha producido un consentimiento por parte de la víctima del acceso a un tercero a la intimidad personal, y este consentimiento inicial modula la pena de

²² Auto de procedimiento abreviado 0001109 /2012, del Juzgado de Instrucción nº 1 de Orgaz (Toledo) en fecha 15 de marzo de 2013.

sólo entre 3 meses a 1 año, contrapuestas a la pena de prisión de 2 años a 5 años cuando se difunden imágenes obtenidas sin el consentimiento. Por consiguiente el legislador debería haber valorado que el daño que produce la publicación de esta faceta de la intimidad personal, aun habiendo consentido su obtención, es muy perjudicial para la víctima y su entorno más próximo, porque la difusión a través de las TIC es absolutamente imparable, y es evidente que el autor que lo ha cometido busca este perjuicio, porque juega muchas veces con las amenazas.

CAPÍTULO IV. DIFICULTADES PARA DETERMINAR LA AUTORÍA, LA COMPETENCIA Y LA PENA DE LOS DELITOS INFORMÁTICOS

El particular funcionamiento de los sistemas informáticos, en unos casos, y los problemas de definición de la titularidad en otros condicionan la atribución de responsabilidad en los delitos cometidos a través de sistemas informáticos o contra éstos. El catedrático MIRENTXU COROCOY BIDASOLOA entiende que además se le suma el problema de identificación de los autores en base al teórico anonimato que proporciona la red, ya que el sujeto pasivo actúa mediante un sistema anónimo como es Internet²³. Desde la perspectiva del Derecho penal material, en particular, en los delitos cometidos a través de Internet, el problema esencial es determinar quién o quiénes son responsables jurídico-penalmente de entre todos los intervinientes. Es necesario saber a quién son imputables los hechos ilícitos, y quiénes son meros facilitadores o tenedores.

Cabe destacar que el factor tiempo, es imprescindible para este tipo de delitos por tres razones, por una parte porque el tiempo es el factor clave para su investigación ya que se precisa una puesta en marcha rápida para poder conseguir que los rastros y pistas técnicas que el autor del delito deja, no se desvanezcan y difuminen en la red. Los datos del tráfico de las comunicaciones desaparecen con gran prontitud, pues la obligatoriedad de su conservación no es igual en todos los países. En Europa se pueden mantener entre 6 meses i 2 años, conforme a la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo²⁴. En España en virtud de la Ley 25/2007 de 18 de octubre, relativa a la conservación de datos de las comunicaciones electrónicas y a las redes públicas de comunicaciones, se establece que en un periodo de normal mínimo de un año, aunque se puede reducir a seis meses o prorrogar a dos años. Y por otra parte el tiempo es fundamental para averiguar la autoría, puesto que la dificultad de ser determinada se incrementa a medida que el tiempo avanza por el hecho que se pueden borrar por el autor del delito los rastros de IP y dificultar así las investigaciones policiales para recabar pruebas.

²³ Mirentxu Corcoy Bidasolo, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos," *Eguzkilore: Cuaderno del Instituto Vasco de Criminología* (Instituto Vasco de Criminología = Kriminologiaren Euskal Instituttoa, 2007), <https://dialnet.unirioja.es/servlet/articulo?codigo=3289399&info=resumen&idioma=SPA>.

²⁴ Velasco Núñez, *Delitos Cometidos a Través de Internet : Cuestiones Procesales*.

I finalmente, para denunciar este tipo de delitos el tiempo también juega un papel clave y es que la prescripción de estos delitos es bastante baja, esto es debido a que la pena que impone el legislador no es muy elevada, produciendo así que su prescripción sea breve y sea un motivo de desestimación de las demandas.

Para determinar la autoría pues, una parte de la doctrina está de acuerdo de plantear la posibilidad de aplicar la responsabilidad en cascada prevista en el artículo 30 del CP, de *lege lata*²⁵ es posible aplicarlo porque Internet es un medio de comunicación aun cuando se suscita la cuestión derivada de la redacción del precepto que limita la aplicación a “*medios o soportes de difusión mecánicos*”. Otra parte de la doctrina entiende que no se podría aplicar porque deja fuera todos los medios de comunicación mecánicos como Internet, Televisión etc. Y finalmente otro sector entiende que no se puede aplicar de forma drástica el precepto porque no es preciso, porque supondría su inaplicación, por tanto se podría aplicar con una interpretación teleológica y no literal del mismo. No hay que olvidar, sin embargo, que el fundamento de este precepto es, entre otras razones, evitar lagunas de punibilidad cuando el autor directo de los hechos no reside en España, cuestión que puede suscitarse en muchos casos en base a la utilización de Internet.

La problemática surge en relación con la posibilidad de atribuir responsabilidad penal por contenidos ilícitos ajenos, es decir, que han sido creados por un tercero. En el ámbito civil y administrativo se han desarrollado sistemas de responsabilidad a nivel europeo a partir de la Dir. 2000/31 CEE, seguida por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico²⁶.

Esta Ley establece las condiciones de responsabilidad dependiendo de las modalidades de intermediación. Primeramente en el artículo 14 establece que la los operadores de redes de telecomunicaciones y proveedores de acceso a las TIC que realizan una actividad de servicio relativa a la transmisión por una red datos facilitados por el destinatario no serán responsables de la información que se transmite. Dicho de

²⁵ Y A N Vera Toste, *Autoría Y Participación*, UNIJURIS, 2015, http://www.lex.uh.cu/sites/default/files/6_VERA_Yan_-_Autoria_y_Participacion.pdf.

²⁶ Cortes Generales, “Ley 34 / 2002 , de 11 de Julio , de Servicios de La Sociedad de La Información Y de Comercio Electrónico . TEXTO CONSOLIDADO Última Modificación : 10 de Mayo de 2014,” 2014, 1–32, <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>.

otra manera, por ejemplo Telefónica Movistar no es responsable de los datos que se envíen por el servicio que presta. En un segundo término nos encontramos con los operadores de servicios que realizan copia temporal, en su artículo 15²⁷, podemos ver como no les atribuye responsabilidad cuando transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, siempre que: primero no modifiquen la información, segundo que permitan el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita, tercero que respeten las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información, y cuarto finalmente que no interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector²⁸.

En un tercer sector, nos encontramos con los prestadores de servicio de alojamiento o almacenamiento de datos proporcionados por el destinatario de este servicio, previsto en el artículo 16, fija que no tendrán responsabilidad siempre que no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. Se entenderá que el prestador de servicios tiene el conocimiento efectivo cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse²⁹.

Y finalmente el último sector que establece son los operadores que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán tendrán responsabilidad por la información a la que

²⁷ Ibid.

²⁸ Corcoy Bidasolo, “Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos.”

²⁹ Cortes Generales, “Ley 34 / 2002 , de 11 de Julio , de Servicios de La Sociedad de La Información Y de Comercio Electrónico . TEXTO CONSOLIDADO Última Modificación : 10 de Mayo de 2014.”

dirijan a los destinatarios de sus servicios siempre que no tengan conocimiento efectivo que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente³⁰

La responsabilidad de los delitos informáticos también se determina en función de la propiedad de los contenidos que vulneran el derecho, por eso la LSSI hace una distinción entre contenidos propios y ajenos. Se entienden por propios no sólo los creados directamente por los prestadores de servicios o intermediarios sino también aquéllos respecto de los que haya originado la transmisión o efectuado la selección de los datos o de los destinatarios de los mismos. No obstante, según el catedrático CORCOY BIDASOLO no se puede pasar por alto que, desde una perspectiva penal, en estos casos se trata realmente de una cooperación en un hecho ajeno³¹. Ahora bien, siempre que se conozca la ilicitud puede hablarse de participación porque el delito no se ha consumado, ya que es necesaria la intervención del prestador de servicios para que esos datos puedan lesionar un bien jurídico, ya sea la intimidad, la indemnidad o la propiedad. En consecuencia, en el proceso de determinación se deberá probar que ese autor desconocido ha realizado un hecho antijurídico.

En cuanto a la difusión de contenidos ajenos las dificultades son mayores y debe plantearse si político-criminalmente es conveniente la intervención del Derecho penal en el control de los contenidos de la Red. En principio, deberíamos partir de la inexistencia de una obligación general de control por parte del proveedor en relación con los contenidos y actividades ajenas, al menos desde la perspectiva penal. Por lo tanto al ser difícil establecer y determinar el círculo de la autoría de estos delitos, no obstante existe también la posibilidad de establecer obligaciones penales de control de esas actividades y contenidos ilícitos, por ejemplo respecto el sujeto pasivo en relación con la pornografía o sexting, se suscitan problemas respecto de la forma de impedir el acceso a menores. En particular, en el supuesto del art. 186 CP, de facilitar material pornográfico a menores, aún cuando se trata de prestadores de servicios, y la solución se ha buscado a través de la exigencia de que esos contenidos no sean de libre acceso y

³⁰ Ibid.

³¹ Corcoy Bidasolo, “Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos.”

estén bloqueados si no eres mayor de edad. En el fondo la misma solución adoptada respecto de las revistas y otros materiales pornográficos, ya que estos no pueden ser comprados por menores de 18 años. Cabe destacar dos cuestiones analizables en la búsqueda de esta solución, la primera duda se plantea si realmente la madurez de los menores de edad se puede establecer mediante la edad física, ya que no todos los mayores de 18 años son suficientemente maduros para entender el contenido. Y la segunda si realmente este bloqueo de contenidos realmente se cumple, o si es fácilmente saltarlos, ya que a la hora de abrirse una cuenta en una red social como Facebook es necesario tener la mayoría de edad pero muchos son los casos en los que los menores están en cuentas de estas redes sociales.

Otro factor clave es la de la competencia de los tribunales, ya que la comisión del delito es a través de internet. Ha habido dudas sobre el foro de competencia judicial. Dado que en muchos casos el carácter anónimo y virtual del ataque, la víctima solo conoce los resultados de la acción, como por ejemplo en caso de recibir un virus no se sabe de dónde procede o quién le ha robado el correo electrónico. En efecto, muchos delitos informáticos, el autor los realiza desde un emplazamiento ignorado a través de un ordenador no fijo, y que puede redireccionar a través de servidores³².

Siguiendo el derecho procesal penal tradicional hay dos teorías las de acción que serían los tribunales del lugar desde donde se ha dirigido el ataque informático, y la teoría de resultado que serían los tribunales del lugar donde se despliega el resultado³³. Para evitar estas discusiones el Tribunal Supremo ha considerado, el principio de ubicuidad, que consiste que el delito informático se produce en todos y cada uno de los sitios donde se manifiestan sus efectos, por lo tanto hace competente *ab initio*, a cualquier juzgado de instrucción cuyo partido judicial se haya evidenciado la exteriorización de cualquier parte del tracto comisivo del delito (STS de 3 de febrero de 2005).

Así mismo, en el ámbito de la delincuencia informática realizada a través de Internet, subsiste la cuestión de si también tiene competencia jurisdiccional el Estado donde se han producido conductas que debemos calificar de cooperación, como son las

³² Velasco Núñez, *Delitos Cometidos a Través de Internet : Cuestiones Procesales*.

³³ Ibid.

de los prestadores de servicios que transmiten datos o seleccionan datos y/o destinatarios. El problema surge desde el momento en que la teoría de la ubicuidad supone una extensión del principio de territorialidad de la ley penal que para algunos plantea problemas político criminales e incluso jurídico-constitucionales. En todo caso, es evidente que de la intervención de diversos Estados en relación con un mismo hecho delictivo pueden surgir conflictos jurisdiccionales de carácter internacional por lo que cada vez son más necesarios los Tratados de Cooperación jurisdiccional tanto en el ámbito de la Unión Europea como a nivel mundial. No hay que olvidar que junto al principio de territorialidad, rigen los principios de universalidad, de protección de intereses del Estado y de personalidad.

Finalmente para la determinación de la pena en casos de concursos de delitos es necesario delimitar cuándo nos encontramos frente a un concurso ideal o real de delitos o, en su caso, frente a un delito continuado. Parece claro que en aquellos delitos que afectan al patrimonio, en sus distintas versiones, estafas, sabotaje informático etc., lo adecuado es aplicar la figura del delito continuado, es importante destacar que se incluyen también los delitos contra la propiedad intelectual, incluso admitiendo que también se protegen derechos morales. Por el contrario, en los delitos contra la intimidad, en principio, no cabe la aplicación del delito continuado, puesto que no se trata de un bien jurídico personal que no se contempla en la excepción prevista en el art. 74.3 CP. No obstante, se podría plantear la analogía entre la excepción prevista para los delitos contra el honor respecto los delitos contra la intimidad. En los delitos relativos a la pornografía infantil y la corrupción de menores cabe la figura del delito continuado, como excepción del art. 74.3 CP. Aplicación que, por otra parte, es jurisprudencia mayoritaria en el ámbito de los delitos contra la libertad sexual en los que las víctimas son menores de 16 años, con independencia de lo criticable que pueda ser este criterio.

CAPÍTULO V. DELITOS CONTRA LA INTIMIDAD PERSONAL, EL HONOR Y A LA LIBERTAD SEXUAL POR MEDIOS INFORMÁTICOS.

Los delitos informáticos que afectan al bien jurídico de la privacidad abarcan como ya se ha establecido en el segundo punto, los derechos del artículo 18 de la CE, concretamente son el honor, la intimidad personal y familiar, el derecho a la propia imagen etc. Debe considerarse que son los delitos informáticos que más perjuicio y daño pueden producir, ya que el nivel de perjuicio de la ciberdelincuencia económica no deja de ser un aspecto económico que con una restitución del daño causado se podría entender que se ha restaurado el perjuicio causado por el delito, en cambio en el caso de violación de la intimidad y contra el honor, el efecto negativo del delito sobre la víctima es imborrable produciendo así un daño irreparable.

Hay distintas formas de cometer el delito de la intimidad, el honor y la libertad sexual mediante nuevas tecnologías de la comunicación, actualmente se engloban diversidad de actuaciones como el sexting, el grooming, el ciberacoso entre otros, pero en este trabajo nos centraremos exclusivamente al estudio del sexting.

5.1. Sexting

El sexting puede ser definido como el envío, normalmente a través de Internet o de un dispositivo móvil, de mensajes con contenido sexual que están producidos y protagonizados por el emisor³⁴. *Prima facie*, la práctica del sexting no suscita interrogantes legales en la medida en que es una práctica voluntaria, mediante la que se comparte un aspecto de la propia intimidad con un tercero, ahora bien la cuestión es que este envío produce una situación de vulnerabilidad de la intimidad para la persona, ya que una vez concluida la relación que unía al emisor y al receptor de esas imágenes puede producir una situación de despecho o diversión emitir esas fotografías de contenido sexual, vulnerando así su privacidad e intimidad

La telefonía móvil se confirma como uno de los servicios TIC con mayor penetración entre la población española. En septiembre de 2009, la Comisión del

³⁴ Martínez Otero, “La Difusión de Sexting Sin Consentimiento Del Protagonista: Un Análisis Jurídico.”

Mercado de las Telecomunicaciones publicaba que el número de líneas ascendía a más de 52 millones, lo que arroja una tasa de penetración de 112,7 líneas por cada 100 habitantes. La extensión de la telefonía móvil alcanza a todas las edades y clases sociales³⁵. Esta tendencia a que el número de líneas de teléfono móvil supere el tamaño de la población del país es frecuente en las sociedades occidentales.

Tal y como ya nos hemos referido, el Sexting es el mero envío de fotografías con contenido sexual entre dos personas. Este hecho no tiene ningún efecto de criminalidad, este efecto nace hace a partir del momento en que estos archivos sexuales, se hacen públicos a través de una red social o a través de algún medio de comunicación vulnerando así la intimidad de la persona, por lo tanto es aquí donde cabe analizar. Parece evidente que la persona sea menor o no, no está percibiendo amenaza alguna contra su privacidad en el momento del envío de estos archivos con carácter sexual, ni es consciente de las implicaciones desde el punto de vista de la seguridad. Algunos expertos consideran que se debe que los adolescentes muestran tal avidez de fama y notoriedad, que les lleva a situaciones que pueden incluso poner en peligro su intimidad, aunque evidentemente los motivos que llevan al menor a enviar esas fotografías son de imposible su conocimiento³⁶.

La palabra sexting es la resultante de la fusión entre dos términos tomados del inglés: *sex* (sexo) y *texting* (envío de mensajes a través del teléfono móvil). En un sentido estricto, el sexting ha sido definido como la “difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico³⁷. Hay diversas características que destacan esta práctica³⁸:

³⁵ Pérez et al., “Estudio Sobre La Seguridad Y Privacidad En El Uso de Los Servicios Móviles Por Los Menores Españoles.”

³⁶ Paz Lloria García, “Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al «sexting»),” *La ley penal: revista de derecho penal, procesal y penitenciario* (Wolters Kluwer, 2013), <https://dialnet.unirioja.es/servlet/articulo?codigo=4654394&info=resumen&idioma=SPA>.

³⁷ José Ramón Agustina Sanllehí, “¿Menores Infractores O Víctimas de Pornografía Infantil?: Respuestas Legales E Hipótesis Criminológicas Ante El Sexting,” *Revista Electrónica de Ciencia Penal Y Criminología* 11, no. 12 (2010): 11, <http://dialnet.unirioja.es/servlet/articulo?codigo=3671649&info=resumen&idioma=SPA>.

³⁸ Martínez Otero, “La Difusión de Sexting Sin Consentimiento Del Protagonista: Un Análisis Jurídico.”

1. Voluntariedad: Es una conducta libre, que no surge del error, la intimidación o la coacción; como mucho, cabría hablar de inconsciencia, ya que los protagonistas pueden no enjuiciar de forma meditada la repercusión que este tipo de imágenes puede llegar a tener dentro de su círculo social o incluso fuera de él.
2. Utilización de dispositivos tecnológicos: El sexting no sería posible sin la existencia de dispositivos tecnológicos que facilitan la captación de las imágenes y su posterior envío. Los dispositivos tecnológicos más empleados son los teléfonos móviles, que permiten captar imágenes en entornos íntimos, así como las webcams pero de forma más residual.
3. Carácter sexual del contenido: Por su propia naturaleza, son contenidos muy conectados con los derechos a la propia imagen y a la intimidad personal.
4. Los archivos tienen naturaleza casera: Frente al carácter profesional de otros materiales provocativos o abiertamente pornográficos, ya sean fotografías o vídeos, el sexting tiene una naturaleza fundamentalmente casera: es producido, protagonizado e inicialmente difundido con una finalidad exclusivamente privada

Es conveniente destacar la diferencia considerada por los cuerpos de seguridad, que hay entre sextorsion y sexting, ya que son dos modalidades distintas. El sextorsion se considera como aquella práctica que se realiza por profesionales que consiste en contactar con personas a través de las redes sociales y conocer su entorno, para conocer a quién le tendrían que enviar las fotografías, obtienen el material pornográfico de forma voluntaria o a través de otros medios, y así extorsionar a la persona para obtener dinero a cambio de no difundir-las³⁹. En paralelo hay la modalidad de sexting que es la que estamos estudiando que suele realizar-se por personas que han tenido lazos íntimos y por despecho o rabia difunde las imágenes para producirle un daño, es evidente que aquí no hay la intención monetaria detrás sino el simple hecho de producir un daño.

³⁹ Ernest Codina (2016) *El «sextorsion» et podria arruinar la vida. Saps què és?* Nació Digital dia 20/03/2016 de : <http://www.naciodigital.cat/noticia/104856/sextorsion/et/podria/arruinar/vida/saps>

En conclusión se entiende por ciberacoso o sextorsion, el conjunto de comportamientos mediante los cuales una persona, un conjunto de ellas o una organización usan las TIC para hostigar a una o más personas⁴⁰. Dichos comportamientos incluyen, aunque no de forma excluyente, amenazas y falsas acusaciones, suplantación de la identidad, usurpación de datos personales, daños al ordenador de la víctima, vigilancia de las actividades de la víctima, uso de información privada para chantajear a la víctima, etc. En todo caso es muy difícil realizar una lista cerrada y definitiva de las formas en las que puede expresarse el ciberacoso. El propio desarrollo de las tecnologías de la información y la comunicación implica que cada poco tiempo los acosadores encuentren nuevas formas de acoso a través de Internet. Esta irrupción, abrupta en la mayoría de casos, trata de poner en evidencia aspectos de su vida personal que la víctima desearía mantener en el ámbito de lo privado, como en este caso el riesgo de que aspectos de la vida íntima como fotos, vídeos o datos privados sean distribuidos entre un número indeterminado de usuarios de Internet es una poderosa herramienta de dominación muy importante, y se diferencia del sexting por el hecho que este delito tiene una finalidad económica.

Por otro lado, también es necesario comparar el sexting con la práctica de el hacking, ya que es la práctica que normalmente se utiliza como vía para cometer el sextorsion, ya que es una práctica consiste en el término que tradicionalmente describe el mero acceso a sistemas informáticos por el gusto de superar las medidas técnicas de seguridad o para la comisión de un delito concreto. Es uno de los delitos informáticos que más frecuentemente se producen. Así, por ejemplo, ya se recogía por la doctrina que en una estadística alemana de 1991, los casos de hacking suponían aproximadamente una quinta parte de todos los ilícitos informáticos, siendo su cifra negra o zona oscura muy amplia y extensa, debido a que a menudo las tentativas de lograr el acceso a un sistema informático no pueden ser constatadas ni advertidas.⁴¹ Se utiliza como vía de realizar el sexting ya que, la entrada al medio de comunicación privado del sujeto pasivo y la difusión del contenido desde esta cuenta, produce una mayor difusión en el entorno de este sujeto. De hecho, la actividad del mero acceso ilegal o ilícito, también denominado intrusismo informático, no tiene para parte de la

⁴⁰ Torres Alberio, Robles, and De Marco, "El Ciberacoso Como Forma de Ejercer La Violencia de Género En La Juventud: Un Riesgo En La Sociedad de La Información Y Del Conocimiento."

⁴¹ Eduardo Escalona Vásquez, "El Hacking No Es (Ni Puede Ser) Delito," *Revista Chilena de Derecho Informático*, no. 4 (March 1, 2011), doi:10.5354/0717-9162.2004.10678.

doctrina una ubicación específica en un área tradicional de bienes jurídicos protegidos, es decir la doctrina tiene diversidad de opiniones para ubicarlo dentro de una tipología de delito u otra, si bien se ha venido entendiendo en el estudio y análisis tal acción ilícita como incidente en el campo de los ilícitos económicos, las respuestas legales en el Derecho comparado lo han venido tratando en otras áreas, principalmente la de los delitos contra la intimidad, como también lo reconoce el propio Convenio sobre la Cibercriminalidad de 2001 es por ese motivo que se trata en este trabajo, porque a partir de este Convenio se entiende delito contra la intimidad personal, al no producir ningún daño patrimonial a la víctima.

Una vez analizado las diversas modalidades delictivas relacionadas, nos centramos otra vez con el sexting, tal y como ya hemos clasificado se encuentra tipificado como una conducta que vulnera el derecho fundamental del artículo 18.1 de la Constitución, relativo al honor y la intimidad⁴². Desde una perspectiva jurídico-penal, el objeto de protección del Sexting es doble, primeramente es evitar la producción de pornografía por cauces que no son los habituales; y por otra parte proteger la deficiente autodeterminación sexual de las personas que realizan este envío de archivos. Respecto a la libertad sexual, conviene señalar que en la inmensa mayoría de países no se reconoce a todas las personas el derecho a decidir mantener relaciones sexuales, dicho de otra manera, se les niega la libertad sexual a los menores a partir de cierta edad (en España, por debajo de los 13 años), por razones vinculadas con su desarrollo y bienestar y, por ese motivo, el bien jurídico protegido en tales casos se denomina indemnidad sexual⁴³.

Se considera pues que dentro del derecho a la intimidad, se encuentra sin lugar a duda, la vida sexual de la persona, tanto en su dimensión estrictamente física o corporal, como en su dimensión más psicológica o sentimental. Por consiguiente, difundir imágenes de contenido sexual de una persona sin su consentimiento supondrá, sin lugar a dudas, una injerencia en el derecho a la intimidad de la persona, al exponer públicamente facetas de su vida que deberían quedar al margen de terceros, aunque la persona que se ha realizado las fotografías haya realizado la difusión al autor del delito.

⁴² Martínez Otero, “La Difusión de Sexting Sin Consentimiento Del Protagonista: Un Análisis Jurídico.”

⁴³ Agustina Sanllehí, “¿Menores Infractores O Víctimas de Pornografía Infantil?: Respuestas Legales E Hipótesis Criminológicas Ante El Sexting.”

La jurisprudencia es variada respecto al entender que se vulnera este derecho, aunque se tiene que tener en cuenta que la gran mayoría es anterior a la Reforma del Código Penal.

Otro derecho que se vulnera con la comisión del sexting es el derecho a la propia imagen, que garantiza a la persona el control sobre la utilización pública de sus cualidades físicas, otorgándole a esa persona el derecho a decidir quién y cuándo puede hacer uso de los mismos, tal i como ha señalado el TC, en la Sentencia 81/2001, de 26 de marzo “el derecho a la propia imagen atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública. La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad -informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde⁴⁴.

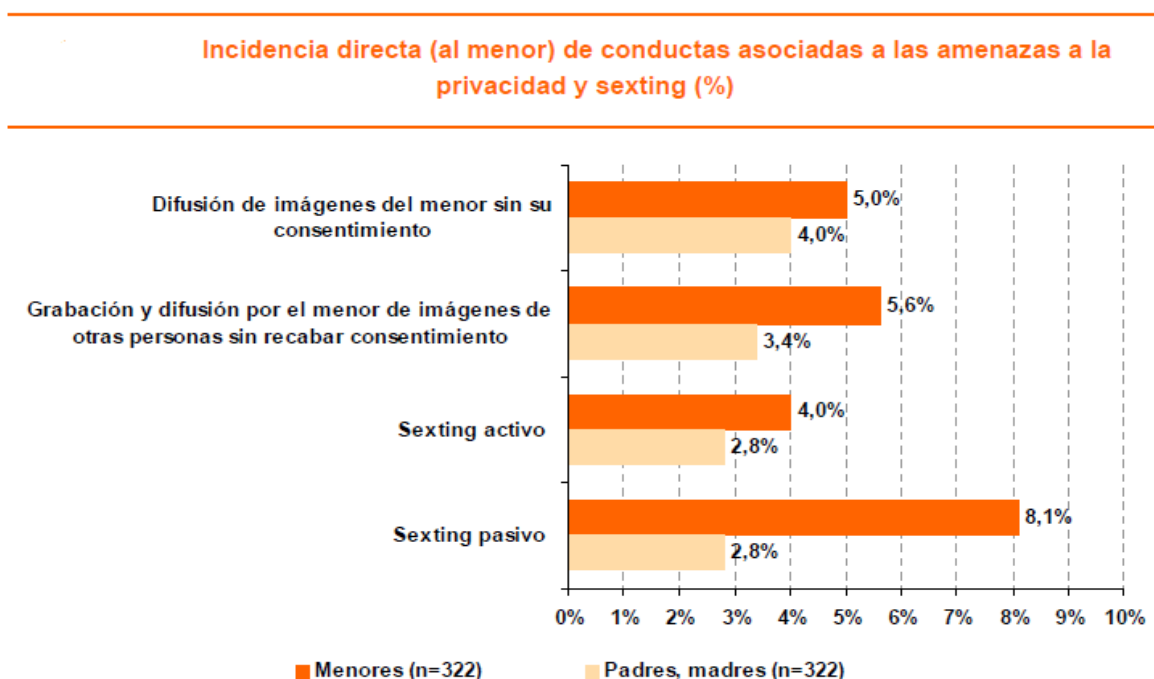
El último derecho que vulnera el sexting, es el derecho al honor del protagonista de los archivos que se difunden en algún medio de comunicación. Este derecho se vulnera si al analizar el contenido de los archivos se incide en la autoestima o la reputación de su protagonista. Primeramente cabe destacar que la consideración de la práctica de relaciones sexuales no es un acto mal considerado por la sociedad, sin embargo los contenidos sexuales que se pueden difundir con el sexting como la masturbación, el exhibicionismo y provocación, si que produce un rechazo y burla social, ergo la publicación de este tipo de contenidos materiales pueden producir una vulneración del derecho al honor, al menos en su dimensión objetiva referida a la imagen pública del sujeto a su reputación o consideración social.

Los adolescentes son más propensos a situaciones de sobreexposición en temas sexuales, especialmente en el entorno cercano entre iguales, ya que son a quienes consideran importantes para su definición y encaje social o pertenencia a un grupo. En los últimos tiempos hemos asistido a una sexualización precoz de la infancia. Este concepto alude a la tendencia por adelantar la adolescencia a edades cada vez más

⁴⁴ Mauricio Menjívar Ochoa, “EL SEXTING Y L @ S NATIV @ S NEO-TECNOLÓGIC @ S : APUNTES PARA UNA CONTEXTUALIZACIÓN AL INICIO DEL SIGLO SEXTING AND NEO-TECHNOLOGICAL NATIVES : Mauricio Menjívar Ochoa EL SEXTING Y L @ S NATIV @ S NEO-TECNOLÓGIC @ S : Mauricio Menjívar Ochoa 1,” *Revista Electrónica Publicada Por El Instituto de Investigación En Educación Universidad de Costa Rica* 10, no. 1409–4703 (2010): 24.

tempranas, y se manifiesta sobre todo en las niñas. El hecho de que las menores adopten conductas sexuales impropias de su edad puede comportar riesgos a nivel psicosocial⁴⁵. Aunque por lo que respecta a la conducta del sujeto activo siempre es dolosa, por lo que si la cesión se produce fruto de una conducta negligente no habrá responsabilidad penal, sin perjuicio de la posible responsabilidad en vía civil. Por lo tanto en caso de imprudencia por parte de la víctima no se entendería un delito penal.

En definitiva el autor de una difusión de imágenes y grabaciones pero no audio únicamente, con contenidos sexuales a través de las redes sociales y/o medios de comunicación, está vulnerando 3 derechos básicos establecidos en la Constitución, el derecho a la intimidad principalmente, a la propia imagen y a la libertad sexual. Aún así los adolescentes no se encuentran del todo concienciados de la problemática y de repercusión de la difusión de archivos con contenido sexual, ya que en el gráfico siguiente se puede comprobar que los adolescentes reciben muchísimos más contenidos de sexting, el llamado sexting pasivo, comparado con a la práctica activa del sexting.



Base: menores (n=322); padres y madres (n=322)

Fuente: INTECO

- Pablo Pérez et al., “Estudio Sobre La Seguridad Y Privacidad En El Uso de Los Servicios Móviles Por Los Menores Españoles,” *Inteco*, 2010, 153.

⁴⁵ M^a Isabel et al., “Guía Sobre Adolescencia Y Sexting : Qué Es Y Cómo Prevenirlo,” *Panorama 1* (2013): 521–34.

Esto se debe, porque es mucho más frecuente que sean ellos mismos los que agranden el problema del sexting, ya que son los propios adolescentes los que realizan más difusión de los propios archivos una vez recibidos. Por todo lo que hemos comentado se debería informar a los jóvenes de toda la problemática de Internet y sobre este tipo de vulneración a la intimidad, ya que la consciencia ante este tipo de prácticas es lo que hará que estos delitos sean menos frecuentes.

Por otra parte, otro dato a destacar es que comprobamos como los padres de estos adolescentes no son conscientes de hasta qué punto su hijo recibe este tipo imágenes, y las difunde mediante las nuevas tecnologías, porque el estudio revela que sólo el 2,8% es consciente de esta incidencia. Esto es bastante preocupante ya que ni los propios padres saben cuáles son los contenidos que reciben sus hijos, que hacen ellos con estos.

Los jóvenes de hoy en día, por su propia naturaleza, están siempre a la última en materia de nuevas tecnologías, conociendo sus límites y explorándose ellos mismos, experimentando la libertad que estas tecnologías lleva consigo. Muchos padres y algunos legisladores han luchado por tratar de mitigar el problema que plantea cómo proteger adecuadamente a los adolescentes ante los nuevos peligros que se derivan de esa libertad digital. En este apogeo de la etapa adolescente, los padres deben tratar de descubrir, ciertamente, cómo educar a sus hijos frente a la creciente comisión de delitos a través de las TIC⁴⁶.

Aunque la típica actitud del adolescente que tiende a explorar en materia sexual no es, en absoluto, un fenómeno novedoso, el amplio uso de Internet, de cámaras digitales, teléfonos móviles y páginas de redes sociales simplemente ha hecho que esta exploración y experimentación sexual adopte distintas formas. No obstante, cuando algunas manifestaciones de curiosidad sexual adolescente son consideradas como normales e inofensivas, en ese momento nos enfrentamos a peligros verdaderamente reales, y no sólo virtuales, como sucede con el Sexting.

Muchos son los casos que se conocen de personas cercanas que han sufrido este tipo de delitos y el hecho que sea tan próximo es alarmante, porque significa que cada

⁴⁶ Ibid.

vez más se encuentra la forma de vulnerar la intimidad de las personas mediante las TIC. Hay que tener en cuenta que la publicación de cualquier contenido en Internet es susceptible de una difusión muy amplia en muy poco tiempo. Y no solo eso, sino que estamos hablando de redes sociales, como Facebook, donde las personas que tiene acceso a la información que cada usuario publica en su “muro” son amigos o conocidos y lo normal es que conozcan a la persona que es retratada, pudiendo visualizar e incluso descargar el contenido audiovisual en el que aparece desnuda o semidesnuda, siendo mayor aún el perjuicio y los daños morales que puedan infligirse a esta.

Asimismo, el Sexting ha sido señalado como una actividad que expone a los adolescentes a medio de presión, como ya hemos comentado del ciberacoso o sextorsion, la explotación y/o ridiculización contra la persona fotografiada e incluso las vejaciones. Cabe destacar que en el caso del ciberacoso, al no existir la presencia física del acosador que se produce en los casos de acoso común, la insistencia en el envío de mensajes se transforma en la fórmula para estar presente en la vida íntima de la víctima y producir así la extorsión de esta⁴⁷. Es por este motivo que en los casos de ciberacoso la acumulación de actividades de acoso, así como el uso de distintas estrategias sea una práctica común y constante⁴⁸. En definitiva la difusión de las imágenes a terceros puede suponer un peligro vital de tal magnitud que se ha relacionado con conductas de intento de suicidio y suicidio consumado, como el caso de una joven de Canadá de 15 años, llamada Amanda Tood que se suicidó en 2012 tras muchos años de cyberbullying y extorsión, por culpa de haberse difundido imágenes con contenido sexual⁴⁹.

Finalmente los expertos consideran que es necesario hacer hincapié en la prevención, y ésta pasa principalmente por inculcar en los menores una cultura de la privacidad⁵⁰. Es decir, conseguir que los menores sean conscientes de los riesgos existentes al exponer datos personales públicamente y valoren la privacidad de sus datos. La medida esencial al respecto es hablar con ellos de forma razonada sobre estos temas, debatiendo los riesgos posibles y los casos de actualidad a la vez que se genera

⁴⁷ Irma Mariana Guti, “Cyberbullying Y Sexting : Percepción Y,” n.d., 93–119.

⁴⁸ Torres Alberó, Robles, and De Marco, “El Ciberacoso Como Forma de Ejercer La Violencia de Género En La Juventud: Un Riesgo En La Sociedad de La Información Y Del Conocimiento.”

⁴⁹ Pantallas Amigas, Video Caso Amanda Tood (2015) Recuperado el día 28/04/2016 des de <http://www.ciberbullying.com/cyberbullying/2012/10/17/el-video-con-el-que-amanda-todd-luchaba-contr-a-el-ciberbullying-subtitulado-al-espanol-por-pantallasamigas/>

⁵⁰ Isabel et al., “Guía Sobre Adolescencia Y Sexting : Qué Es Y Cómo Prevenirlo.”

un ambiente de confianza que facilite que el menor exponga sus ideas y problemas y así reflexione sobre las posibles consecuencias.

5.1.1. Sujetos del delito

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos.

En el caso del sexting el sujeto activo es aquel que ha obtenido, con el consentimiento del sujeto pasivo, imágenes o grabaciones audiovisuales de éste. Ciertamente el sujeto activo que comete este tipo delictivo, es una persona del círculo cercano de la víctima que ha mantenido o mantiene una relación con ella, ya que si no parece evidente que la víctima no habría accedido a la cesión de dichos archivos de contenido íntimo. En la actualidad estas personas que deciden producir un daño a una persona de su confianza, han crecido ya que se esconden utilizando medios informáticos debido a la gran utilización de las TIC, y causando el mayor daño posible debido a su rápida difusión. Por lo tanto se ha vuelto un instrumento de revancha.

El legislador ha limitado el círculo de los posibles autores a aquel o aquellos que efectivamente han captado o recibido imágenes de la víctima, bien porque directamente el sujeto activo las haya realizado, o bien porque la propia víctima le ha proporcionado.

Por consiguiente quienes produzca la divulgación contribuyan a la posterior difusión, no tienen responsabilidad penal, pero si tienen responsabilidad civil a través de la LO 1/1982, aunque evidentemente es sumamente complicado comprobar quien ha difundido esta imagen una vez se ha difundido en una red social, ya que como ya hemos dicho aunque la difusión pública a través de internet los contenidos se pueden descargar y difundirlos por medios de comunicación más privados como WhatsApp o correo electrónico.

Finalmente por lo que respecta el sujeto pasivo, es aquel cuya imagen es fotografiada o grabada, que da su consentimiento para que el archivo se realice en un

contexto de intimidad pero que no autoriza al sujeto activo la difusión a terceros de estos. Este tipo de prácticas suelen llevarse a cabo en un contexto como ya hemos dicho de relación sentimental, en la confianza del consentimiento mutuo al envío de fotografías, y con el convencimiento que la imagen o grabación no va a salir de dicho círculo íntimo. Por ello el consentimiento del sujeto pasivo solo alcanza a la recepción por el otro participante en la relación, y no se extiende a la divulgación que tiene lugar con posterioridad.

Es importante para finalizar destacar la diferencia entre los sujetos activos de la práctica delictiva del sexting con los del sextorsion, ya que mientras el sexting es el círculo cercano de la víctima y por lo tanto se hace con la intención de producir un daño a esta, el sextorsion es un profesional que tiene un interés económico y no con el interés propio de dañar a la persona en concreto sino que tienen diversos sujetos extorsionando a la vez.

CAPÍTULO VI. UNIDAD CENTRAL DE DELITOS INFORMÁTICOS DE LOS MOSSOS D'ESQUADRA

La unidad central de delitos informáticos, es una unidad de la Área Central de Investigación – Personas que se ocupa de los casos criminales que tienen lugar en las redes de internet y ofrecen soporte técnico a las otras unidades de investigación del cuerpo de los Mossos d'Esquadra. El área Central de Investigación de Personas, es la unidad que se encarga, tal y como establece el artículo 21 del *“Decret 415/2011, de 13 de desembre, d'estructura de la funció policial de la Direcció General de la Policia”*; a la investigación de los delitos que afectan a la vida, o salud de las personas y aquellas actividades realizadas por grupos juveniles organizados.

Los orígenes de la unidad se remontan al 1997. Una de sus intervenciones más relevantes se produjo el 27 de mayo de 2011, ya que colaboraron para proteger los sistemas informáticos de la Generalitat de Cataluña que estaban siendo víctimas de ataques masivos utilizando redes zombis de todo el planeta.

Esta Unidad central está especializada y se encarga de la investigación de una amplia variedad de casos y a la vez también tiene la función de garantizar la seguridad de determinados sistemas informáticos. La criminalidad que se produce a través de la red más común según este departamento, son las compras fraudulentas mediante obtención de datos personales, las suplantaciones de identidad, el acoso y el chantaje a menores, la pornografía infantil, el cyberbullying, el blanqueo de capitales, el sexting, las estafas etc.

Otro campo importante de actuación son los ataques cibernéticos, en sistemas públicos de la Generalitat, porque cada mes reciben una mediana de 500.000 ataques o intentos de intrusión, o de manipulación de datos. Aunque los ataques más peligrosos son los que pretenden vulnerar las infraestructuras críticas del país, como centrales eléctricas, nucleares, telefónicas etc. Cabe remarcar que atacar una red informática cerrada es un delito penal de hasta 4 años de prisión.

Una vez analizado de forma breve las funciones más destacadas de la unidad central y sabemos a qué se dedica el Sr. JORDI DOMÈNECH podemos adentrarnos al delito concreto del sexting y preguntarle sobre las funciones de los cuerpos policiales para controlar esta problemática.

Llego a la Central de los Mossos d'Esquadra, un edificio muy grande y con vidrio, realmente impresiona al verlo. Una vez allí entro dentro y me facilitan una acreditación. Me viene a buscar el Sr. Jordi Domènech, se le ve una persona muy cercana y amable, nos saludamos y me enseña las instalaciones que forman la Central. Subimos a la segunda planta y vamos a su despacho, bastante grande y luminoso, nos sentamos y comenzamos la entrevista.

¿En qué año entró a formar parte de la Unidad Central de Investigación de personas de los Mossos d'Esquadra?

Complicado, porque he entrado y salido de la Unidad varias veces, pero entré en el año 1990 al Cuerpo de los Mossos. En 1992 empecé en la policía judicial y estuve temporadas largas de investigación en Girona, Manresa, Barcelona y en Servicios Centrales ... pero fui ascendiendo hasta ser inspector adscrito a la Unidad de Fiscalía del TSJC y posteriormente en 2009 me hice cargo de la Unidad Central de Investigación de personas. Puede parecer pocos años, pero llevo muchos años entrando y saliendo de los departamentos de investigación.

El Departamento Central de Delitos Informáticos forma parte de esta Unidad, ¿qué delitos informáticos suelen investigar?

En principio todos los delitos que se consideran especializados, todos aquellos delitos que el territorio no puede investigar porque necesitan una cierta capacitación vienen a parar aquí, siempre que sean de tipología informática. Podemos decir que todos los delitos que se consideran informáticos, desde delitos contra el patrimonio, o acosos, amenazas...cualquier delito del código penal que se hayan utilizado herramientas informáticas. Es que esto ha cambiado mucho, antes eran delitos tecnológicos, ahora se consideran delitos informáticos y pronto no tardarán en decirse delitos de Internet. Son

delitos telemáticos que se producen a través de Internet, se investiga principalmente la red de las redes, por lo tanto cualquier delito que se produzca por Internet se puede investigar, desde un sicario que se ofrezca por matar a otro, encontrar bienes sustraídos, espionaje industrial...y concretamente nosotros estudiaremos los más difíciles de investigar.

Hay estudios que revelan que los delitos informáticos han experimentado un fuerte crecimiento, ¿el Departamento de Investigación ha notado este crecimiento con el aumento del n° de denuncias?

Sí exactamente, va creciendo conforme más se utiliza la Red, todo el mundo está conectado a la red. Antes Internet sólo se podía tener a la vivienda, ahora actualmente todo el día estamos conectados, no sólo es el correo electrónico sino es la calefacción que se conecta con vía telemática, el control de cámaras...nos encontramos cada vez más conectado a Internet. Hemos ido experimentado un aumento exponencialmente de estos delitos, ya que cualquier delito se puede cometer a través de Internet. Internet da ventajas para hacer una serie de delitos sobre todo los que provocan un engaño, ya que es mucho más sencillo engañar, principalmente estafas y acoso a menores, con todas las ventajas que implica como estar haciendo el delito en la otra punta del mundo, realizar microestafas porque no se suele denunciar ya que son cantidades pequeñas de dinero. Por lo tanto todas las nuevas modalidades delictivas.

Centrándonos con el Sexting, ¿qué perfil suelen tener las víctimas? ¿Y los autores de los delitos?

Debemos diferenciar entre Sextorsion y Sexting. En cuanto el Sextorsion es la persona que expresamente engaña a otra persona para que realice imágenes eróticas o pornográficas para extorsionarla para obtener algún beneficio económico. Y en cuanto al Sexting lo entendemos como aquella difusión de imágenes de una persona que tenía una relación consentida previa con el autor del delito, y este publica los archivos con la intención de hacer daño porque esta relación se ha roto. Por lo tanto en el primer caso hablamos de personas profesionales en la extorsión y en cambio el sexting son motivos personales. En cuanto al sexting se produce porque ha cambiado la forma de entender las relaciones y los medios para grabar, ahora se cuelga y se graba todo, se debería

estudiar cómo se registran estos archivos y cómo se graban. Antes enseñabas una fotografía y volvía a ser tuya, actualmente la fotografía se da, y se dan vídeos... ahora damos todo, incluso se da la intimidad.

En cuanto el Sextorsion el autor no lo hace para hacerte daño, sino para obtener un rendimiento económico, por lo tanto es un profesional con un motivo exclusivamente económico, no tiene interés para hacerte daño. Y ante estos delitos nos encontramos normalmente autores Sur-africanos, concretamente de Nigeria. Estas personas se dedicaban normalmente a hacer estafas, las llamadas Cartas Nigerianas y actualmente a extorsionar. Suelen ser hombres que se hacen pasar por mujeres, para engañar a un hombre teniendo una relación sentimental, así conocen su entorno y para conseguir imágenes, y una vez las tiene hacer la extorsión que si no obtiene dinero las difundirá a su entorno. Estos delincuentes al mismo momento tienen carpetas de la información de las personas que recopilan, y para posteriormente extorsionarlas, crean una maquinaria de hacer extorsiones.

En cambio con respecto el Sexting son hombres que amenazan que si no vuelven difundirán las imágenes o las cuelgan directamente. Normalmente nos encontramos con hombres que para intentar volver con la ex pareja la amenaza, pero son amenazas cotidianas, no dinerarias.

¿Los Mossos d'Esquadra actualmente realizan algún tipo de charla informática para prevenir este delito?

Intentamos hacer campañas para que los jóvenes sean más conscientes de los riesgos de la Internet, pero cuesta mucho hacerlas y concienciar que realicen cambios en sus hábitos de vida con Internet.

En caso de que un adolescente denuncie un caso de divulgación de fotografías de este tipo ¿Cómo se actúa desde los Mossos? ¿Cómo se realiza la recopilación de diligencias de investigación?

Cuando se tiene una denuncia de este tipo de sexting, aunque no es demasiado común hay muchas más denuncias de Sextorsion, primero la víctima tendría que determinar quién ha tenido acceso a estas fotografías ya que si la fotografía o el vídeo ya la ha difundido a muchas personas no hay delito. Pero si realmente sólo hay una persona ante la que haya accedido a darle los archivos y está identificada, y éstos se han difundido pues esta persona tendrá que dar explicaciones. A partir de aquí se debe investigar si él las ha difundido a una persona y es esta la que ha cometido el delito, o si le robaron las fotografías, o si realmente las ha difundido, es que de posibilidades hay muchas. En caso de que no esté identificada se debe hacer una comisión rogatoria internacional del juez, ya que estaríamos en otra jurisdicción ya que casi todas las redes sociales normalmente se ubican en Estados Unidos. Por lo tanto la red social de donde se ha difundido te haga llegar la IP y se empiece la investigación. El problema es que el juez ya no realiza esta comisión rogatoria para modalidades delictivas como éstas.

¿Suelen ser condenadas las personas que cometen este delito?

Por estos delitos podrían ser condenadas, pero es que son delitos muy leves. Todo los casos que son de violación de la intimidad, o de injuria para saber nosotros quien ha cometido el delito tal y como ya te he comentado son plataformas Americanas y es complicado conocer el autor. Para la víctima puede ser es importante pero en Estados Unidos no es un delito tan importante, ya que alegan con frecuencia la libertad de expresión para justificarlo, y además, es difícil que el Juez realice la comisión rogatoria, y en caso de que el juez la realice, que la plataforma acepte ceder la identidad del autor, por lo tanto encontramos muchas peticiones negativas. Ahora bien para delitos graves como terrorismo o por temas de secuestro todos los países suelen colaborar. Pero para una foto o un vídeo pornográfico que no se ve maltratos, nos encontramos muchas dificultades para que estas peticiones prosperen. Y estamos hablando de investigaciones donde no se han utilizado mecanismos de borrar los rastros que entonces aún se complica mucho más la investigación.

***¿Hay alguna dificultad si el autor de este delito es de fuera del territorio catalán?
¿Cómo se coordinan con otros cuerpos de policiales?***

El autor es muy complicado, pero en caso de que sea un acoso de Whatsapp o correo que utiliza todos los medios para amenazar a la pareja sí sería sencillo, ya que las parejas son en principio dentro del ámbito de proximidad. Pero cuando hablamos de delitos de base internacional, se complica mucho, los autores del delito que no sabes dónde está esa persona, es realmente muy complicado. Cuando nos llega una IP que no se encuentra en España, ya sabemos que hasta aquí hemos llegado, porque necesitamos legislación internacional y mucha más colaboración internacional, porque Internet sobrepasa fronteras.

Normalmente antes de que se produzca esta divulgación se producen amenazas, para forzar alguna actuación de la víctima, ¿los Mossos podrían actuar para prevenir la difusión posterior, en estos casos?

Sí que podríamos actuar, no hace falta colgar las imágenes. Es decir una vez te amenazan que las fotografías serán difundidas ya se podría actuar siempre y cuando esté un poco fundamentada. Si se produce una amenaza y el autor ya se conoce, ya se le imputaría el delito, antes de que lo haga, pero si ya lo ha se le imputaría la revelación de secretos.

La legislación siempre es más lenta que las nuevas formas de actuación de los delincuentes, es por eso que esta práctica no estaba regulada hasta la última Reforma del CP que la ha incluido en el delito de revelación de secretos previsto en el artículo 197.7 del CP. La pena es de entre 3 meses a 1 año, ¿la considera suficiente?

No, no está. Esto pasa igual que el ciberbullying, ya que no es lo mismo sitió un niño solo en la escuela que sólo lo ven los niños del patio de la escuela, que hacerlo por Internet que lo ve todo el pueblo.

A parte de que todo lo que entra en Internet es para toda la vida, solamente que una persona guarde la fotografía o vídeo en su disco duro, al cabo de unos años en cualquier momento lo puede volver a colgar y volverá a estar esparcido por la red. Una vez se

pasa a otra persona y se difunde el archivo, siempre se tiene el temor de que este archivo se vuelva a colgar. Este mal siempre estará, esta sombra siempre estará, se pueden utilizar medios para sacar el vídeo o fotografía que no se vea pero siempre existe la posibilidad de que se vuelva a colgar a demás que siempre necesitarás a alguien que esté limpiando tu imagen. Y aún más si las imágenes son con contenido pornográfico ya que hay plataformas muy grandes que recogen pornografía que tienen bases de datos muy grandes, puede que desaparecen pero vuelven a aparecer al cabo de unos años. Nosotros podremos actuar pero se necesita la denuncia para intentar frenarlo, porque es difícil saber si se voluntario o no, ya que en ese momento la víctima no era consciente y parece que está bien, es cuando el otro lo difunde sin el consentimiento de éste cuando hay el mal.

¿Cree que a pesar de la última Reforma Penal el legislador está regulando correctamente las prácticas delictivas a través de las TIC?

En general el tema de delitos informáticos contra la intimidad deberían ser penados más todos, como los delitos de amenazas, injurias, calumnias...pero bastante más, porque Internet replica y replica, y se expande. La información que se cuelga en Internet no se comprueba, todo el mundo opina y todo el mundo dice sin ninguna forma de contrarrestar esta información. Debemos ser conscientes de que no todo lo que sale en Internet es veraz, se debería regular.

¿Finalmente considera que las medidas de actuación de la policía se ven limitadas por la legislación actual?

Deben poner unas herramientas para que la policía pueda trabajar en el tema de Internet o cada vez se podrá hacer menos en estos delitos. Si la comunicación se hace de forma encriptada y se ponen trabas para que la policía conozca la identidad de los delincuentes aumentan y mucho, es que ya no es que sea difícil saber quién está detrás, sino que las empresas no facilitan la información y no podemos intervenir. Los delincuentes lo saben y la policía no podemos acceder. O se les obliga a que para funcionar la policía pueda acceder a esta información con la correspondiente autorización policía, o no podremos investigar.

Si queremos proteger a las personas y seguridad, la libertad de expresión no debe servir para todo, la policía debe tener medios para poder acceder a la información de quien se registro en las redes sociales. Deberíamos saber el DNI y saber quién ha publicado las cosas, no es que salga publicado en la Red Social, pero sí que si esta persona realiza algo de estas no se puede saber.

Los mecanismos para identificar a las personas que tienen estas plataformas no dan la identidad sino simplemente un IP, que no sabes realmente quien se ha conectado a esta plataforma. Según qué delitos ya no dicen quién está detrás porque se entiende como libertad de expresión, el problema de Internet son los casos leves que aunque para ti te afecte, los jueces no dan la comisión rogatoria que él debe hacerla con inglés y todo, y por tanto se queda en nada.

Lo más importante es que la intimidad de las personas cada vez se difunde más, todo se cuelga y dentro de unos años esta fotografía te puede perjudicar. Antes esta foto era tuya ahora actualmente no sabes a donde llega o al que llega. Puedes haber ceder fotografías que antes eran tus actualmente se difunden con mucha facilidad, ahora mismo se apretar una tecla.

Debemos actualizarnos con la tecnología y modificar nuestros hábitos

CAPÍTULO VII. ANÁLISIS DE UN CASO PRÁCTICO

Una chica de 16 años, llamada Raquel S. residente en Tarragona, sin antecedentes penales, conoce a un chico de 19 años a través de una red social, llamado Iván B. residente en Arcos de la Frontera, ya que él la añade a la red social. Empiezan a hablar durante unos meses hasta que Iván, sin antecedentes penales, le empieza a enviar fotografías con contenido sexual. Raquel a su vez le responde enviándole el mismo tipo de archivos. Hasta que un día Raquel después de 1 año y medio, queriendo dejar de hablar con Iván, conoce a Pablo G. y empieza una relación estable, esto hace que Iván se enfurezca y empiece a amenazar a Raquel repetidamente que si no deja esta relación publicará las fotografías que le había enviado en su red social. Iván tiene conocimientos informáticos así que piratea el correo para poder entrar en la red social Facebook de Raquel y desde su red social publica las fotos para que todos sus contactos puedan descargar los archivos y comenten produciendo así un bochorno y vergüenza de Raquel. Ella se guarda todos los correos electrónicos que prueban las amenazas que Iván le dirigió. ¿Cuál será su pena?

En este caso concreto encontramos tres delitos cometidos, el primero es el de revelación de secretos previsto en el artículo 197.7 del Código Penal, el segundo el delito de Amenazas previsto en el artículo 169, y finalmente el delito de vulneración de seguridad para entrar en un sistema informático sin estar autorizado previsto en el artículo, conocido como hacking 197 bis del Código Penal.

Por consiguiente bien jurídicamente protegido es la intimidad personal y la libertad sexual. También podríamos incluir el derecho al honor previstos en el artículo 18 de la CE.

En lo referente a los sujetos, encontramos al sujeto activo que en este caso es Iván B. quien difunde los archivos, amenaza e se introduce en un sistema informático sin consentimiento.

Por lo que se refiere a la parte objetiva, hay que analizar dos aspectos:

- Relación de causalidad: cabe analizar si la acción realizada por el sujeto activo es realmente la causante de diferentes delitos como en este caso son la revelación de secretos, las amenazas y el intrusismo a un medio de comunicación privado. Por lo tanto comprobamos que sí que la actuación de Iván B ha causado la lesión al bien jurídico protegido
- Imputación objetiva: en relación a la imputación objetiva, cabe analizar tres aspectos: el peligro jurídicamente desaprobado, constituyen unas prácticas penalmente estipuladas como ilícitas en el Código Penal; peligro previsible, claramente la acción produce un peligro al bien jurídico protegido de la intimidad; y finalmente la concreción de ese peligro en el resultado, se ha vulnerado el derecho a la intimidad y la libertad sexual.

En referencia a la parte subjetiva es evidentemente una práctica dolosa, ya que las amenazas, el descubrimiento y revelación de secretos y el hacking son delitos que solo se pueden realizar mediante una acción dolosa, dicho de otra manera las diferentes acciones que se llevan a cabo tienen la finalidad de llevar a cabo el delito que se ha cometido. Concretamente es un dolo directo ya que la persona que ha cometido el delito dolos, tal y como se produce en el presente caso, conocía y tenía la intención de llevar a cabo el delito con su acción que el resultado de estas acciones sería la materialización en un riesgo ilícito para producir unas lesiones en un bien jurídico. Por lo tanto Iván B. con esta acción conocía perfectamente que produciría una lesión a la intimidad de Raquel S.

En este caso aparentemente no hay causas de justificación del delito, como la legítima defensa, el estado de necesidad, el consentimiento o el cumplimiento de un deber.

Por lo que respecta a la culpabilidad no se encuentran motivos de inimputabilidad o de error de prohibición por parte del autor del delito.

La determinación penal a través del marco abstracto:

- Delito de amenazas establecido en el artículo 169.1 del CP, con una pena prevista de 1 a 5 años de pena privativa de libertad, con un agravante a su

mitad superior porque estas se han realizado mediante un medio de comunicación como es el correo electrónico.

- Delito de revelación de secretos establecido en el artículo 197.7 del CP, con una pena prevista de 3 meses a 1 año de pena privativa de libertad.
- Delito de entrar en un medio de comunicación prevista en el artículo 197 bis del CP, con una pena prevista de 6 meses a 2 años de pena privativa de libertad.

Por lo que respecta al Marco concreto, cabe analizar si los tres delitos se han consumado o no, y en este caso los tres se han consumado por lo tanto no nos encontramos frente al grado de tentativa prevista al artículo 62 CP. En referencia al grado de participación, el autor del delito es el Sr. Iván B. y no se puede imputar en grado de complicidad previsto en el artículo 63 CP a los que una vez las fotografías son publicadas las difunden. No se contemplan causas agravantes o atenuantes de la responsabilidad previstas en los artículos 21 y 22 CP por lo que no se modifica la pena tal y como se prevé en el artículo 66 CP. Y finalmente no se contemplan eximentes incompletos de la responsabilidad penal previstos al artículo 68 CP.

La pena se tendría que calcular en base a un concurso medial de los delitos de vulneración de secretos y el de entrada ilícita a un medio de comunicación, y un concurso real con el delito de amenazas. Esta consideración es en base a que la entrada a la Red, sirve como medio para poder cometer el delito y así llegar al entorno más próximo de la víctima, y sería el concurso real con el delito de amenazas.

A modo de conclusión cabe destacar que llama la atención que el delito más grave sea las amenazas correspondiente al artículo 169 CP, ya que en base a el daño que puede llegar a causar el sexting comparado con las amenazas, es fácilmente considerable que las penas son completamente incoherentes. El daño a la intimidad que produce la vulneración de la intimidad sexual es completamente superior al daño que produce que te amenacen que van a producir un perjuicio, ya que uno es un hecho real y el otro una posibilidad de realizarse, por eso se tendría que imponer una pena más superior a este tipo delictivo por mucho que la víctima haya consentido la entrega de esta intimidad a esta persona, entendiendo pues que este consentimiento se produce

siempre con personas que tienes un especial vínculo efectivo entre el autor del delito y la víctima, y que por lo tanto se tendría que modular.

No se puede entender como el legislador ha impuesto una pena tan baja para una vulneración de tal calibre, y en cambio en el delito previsto en 197 bis que es el simple hecho de entrar en un sistema de comunicaciones sin la autorización de la víctima tiene una pena de prisión de el doble de años. Es un error grave que se produzca esta falta de consideración por parte del legislador de estas personas que por un mero consentimiento, tengan que soportar que el delito que realmente les produce el daño más importante sea el que menos pena establece.

CAPÍTULO VIII. CONCLUSIONES

Primera. Una vez analizados los aspectos jurídico-penales del delito de sexting y la evolución que se está produciendo en los delitos informáticos, cabe destacar diversos aspectos. Por una parte, es claramente apreciable que los delitos contra la intimidad a través de las TIC, tienen más repercusión y son más frecuentes en la actualidad, la facilidad de cometer estos delitos y sobretodo la repercusión social que tienen en la vida de la víctima es lo que impulsa a los autores a cometerlos.

Segunda. En el trabajo presentado, nos hemos referido a una tipología de hechos que se dan con una incidencia que aún no es muy notable, sin embargo, es lógico pensar que irán en aumento en los próximos años, precisamente por el uso generalizado, la conectividad permanente y la emergencia incontrolable de programas y plataformas en estos dispositivos móviles y el incremento a una mayor exposición de riesgo, especialmente en edades inferiores, por el descenso de la edad en que se inicia su utilización.

Tercera. Otro punto que cabe destacar es la impunidad de estos delitos si eres mayor de 17 años y si has consentido que un tercero interfiera en tu vida íntima, se establece en el artículo 197.7 del CP una pena privativa de libertad de entre 3 meses y 1 año. Evidentemente es prácticamente imposible que este sujeto cumpla esta pena privativa de libertad porque es ínfima, en comparación con otros delitos, y esto produce que sea una práctica fácilmente realizable porque las consecuencias jurídicas que tiene son escasas. Y aún hay más, hasta la última reforma del Código Penal de 2015 era una conducta únicamente de la jurisdicción civil, es decir, no se establecía relación penal, cuando es evidente que el daño al bien jurídico de la libertad sexual e intimidad personal existe. Aunque la víctima consienta que las fotografías o grabaciones se realicen, no consiente para que estas se difundan, y menos entre las personas de su entorno próximo, por eso no es lógico que no se introdujera en el código penal. La única voluntad del autor de este delito es causar un daño a su intimidad personal, ya que conocen perfectamente que la sociedad ante este tipo de fotografías personales realiza burlas y cuchicheos.

Cuarta. El legislador tendría que ser más consciente que la voluntad de realizar un daño es importante, y que este daño es efectivamente causado. Cuesta entender por qué en el caso de menores de 16 años esta pena se considera pornografía infantil y a partir de esa edad ya es considerado que se consiente y la pena que se debe aplicar es mucho más baja. La realidad actual es que el sexting es una práctica entre jóvenes y adolescentes, de entre 13 y 18 años. Durante esta edad es fácilmente considerable igual de inmaduro un menor de 16, que uno de 16 y un mes, o uno de 17 años, porque realmente la edad física no influye en la madurez de una persona, y en consecuencia a la toma de decisiones como es el consentimiento de este tipo de prácticas.

Quinta. Por otro lado es obvio que hay una actitud inconsciente de la víctima, porque evidentemente un archivo con contenido sexual es un arma para amenazar, y la víctima no es consciente debido a la confianza que existe entre los dos sujetos. El sexting siempre sigue el mismo patrón, existe una relación mutua entre el sujeto activo y pasivo, el sujeto pasivo consciente durante la relación el hecho de realizar fotografías o grabaciones con contenido sexual, y cuando este decide poner fin a la relación, el sujeto activo amenaza que se producirá esta difusión para que todo el mundo, y básicamente su entorno próximo sepa qué clase de mujer es, ya que se producen muchos más casos en mujeres que en hombres. Desde mi consideración la advertencia a los jóvenes es importantísima para que no se realicen ningún archivo de este tipo ergo esto es clave para que el sexting se frene, porque si la víctima no consintiera, ya no habría posibilidad de dañar su intimidad. También sería conveniente intentar concienciar el daño que se produce a la persona, ya que cómo ya hemos comentado a veces el daño se produce con más magnitud cuando los propios jóvenes difunden por otros medios los archivos con este tipo de contenido, porque entonces se hace viral y el daño a la víctima es claramente superior.

Sexta. Para finalizar este trabajo y a modo de conclusión considero que conocer la experiencia de las personas es fundamental, ya que te acercan al hecho delictivo y al daño que le ha causado, es por eso que quiero incluir una breve referencia a esta problemática creciente del sexting, desde mi experiencia personal. El daño que causa no es comparable con nada, ya que destruyen toda confianza que puedes tener en ti en un breve instante. El momento en el que las personas son testigo del contenido de los archivos y suena el teléfono preguntando lo que sucede en la red social, no se borra de

la mente, ni mucho menos la sensación de como se bloquea cada parte del cuerpo y una corriente de calor sube por el mismo, y por la cabeza pasan multitud de ideas. En mi caso muchos decían que me tendría que ir de la ciudad y dejar los estudios que estaba cursando, aunque te lo llegas a plantear, es de cobardes hacerlo, el hecho está allí quieras o no, y si decides la opción fácil nunca se supera, por eso en una semana estaba en el instituto y actualmente terminando mi Grado sin haber desperdiciado un solo año de mi vida por este hecho. Aún así, considero que las personas deberían ser conscientes que la intimidad personal vale mucho más de lo que se considera en general, y no se debe dejar por nada del mundo que te la arrebaten como en mi caso me han hecho.

Séptima. En definitiva, respondería a la pregunta de si la persona que ha sufrido el sexting es víctima o inconsciente, diciendo que las personas son por un lado víctimas del delito, pero a la vez inconscientes de haber creído en una persona y haber dejado que se inmiscuya en su intimidad, por eso cabe despertar la consciencia de nuestros jóvenes, primero para evitar que eviten el exhibicionismo y en segundo lugar para poder evitar que estos casos sirvan para que se fomente el acoso a una persona, porque cuesta entenderlo pero la raza humana siempre acostumbra a hacer más daño al que se sabe que está débil y en tercer lugar a entender que las fotografías actuales si se cuelgan no se enseñan sino que se entregan y en consecuencia estas nunca más van a ser privadas.

BIBLIOGRAFIA

- Aguilar Cárceles, Marta María. "Cybercrime and Cybervictimization in Europe: Institutions Involved in Cybercrime Prevention in the United Kingdom." *Revista Criminalidad* 57, no. 1: 121–35. Accessed March 5, 2016. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082015000100009&lng=en&nrm=iso&tlng=es.
- Agustina Sanllehi, José Ramón. "¿Menores Infractores O Víctimas de Pornografía Infantil?: Respuestas Legales E Hipótesis Criminológicas Ante El Sexting." *Revista Electrónica de Ciencia Penal Y Criminología* 11, no. 12 (2010): 11. <http://dialnet.unirioja.es/servlet/articulo?codigo=3671649&info=resumen&idioma=SPA>.
- Cisternas Hernández, Emilio; "Análisis Y Proyección de Los Delitos Informáticos En Chile." *Universidad de Talca* 53, no. 9 (2013): 72. doi:10.1017/CBO9781107415324.004.
- Comes Raga, Ignacio. "La protección penal de la intimidad a través de la difusión in consentida del sexting ajeno." *La ley penal: revista de derecho penal, procesal y penitenciario*. Wolters Kluwer, 2013. <https://dialnet.unirioja.es/servlet/articulo?codigo=4654389&info=resumen&idioma=SPA>.
- Corcoy Bidasolo, Mirentxu. "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos." *Eguzkilo: Cuaderno del Instituto Vasco de Criminología*. Instituto Vasco de Criminología = Kriminologiaren Euskal Institutoa, 2007. <https://dialnet.unirioja.es/servlet/articulo?codigo=3289399&info=resumen&idioma=SPA>.
- Escalona Vásquez, Eduardo. "El Hacking No Es (Ni Puede Ser) Delito." *Revista Chilena de Derecho Informático*, no. 4 (March 1, 2011). doi:10.5354/0717-9162.2004.10678.
- Fiscalía. "Instrucción 2/2011 Sobre El Fiscal de La Sala de CRIMINALIDAD INFORMÁTICA Y LAS SECCIONES DE CRIMINALIDAD INFORMÁTICA DE LAS FISCALÍAS," 2011, 2074–94.

- Gerke, Marco. "The Global Challenge." *Population Reports. Series M. Special Topics*, no. 15 (2000): 1–2.
- González Cussac, José L., Ángela Matallín Evangelio, and Elena Górriz Royo. *Comentarios a La Reforma Del Código Penal de 2015*. Valencia : Tirant lo Blanc, 2015. http://cataleg.urv.cat/record=b1496059~S13*cat.
- Guti, Irma Mariana. "Cyberbullying Y Sexting : Percepción Y," n.d., 93–119.
- Isabel, M^a, Fajardo Caldera, Marta Gordillo Hernández, Ana Belén, Regalado Cuenca, Inteco, and Jorge Flores Fernández. "Guía Sobre Adolescencia Y Sexting : Qué Es Y Cómo Prevenirlo." *Panorama 1* (2013): 521–34.
- Lloria García, Paz. "Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral (especial referencia al «sexting»)." *La ley penal: revista de derecho penal, procesal y penitenciario*. Wolters Kluwer, 2013. <https://dialnet.unirioja.es/servlet/articulo?codigo=4654394&info=resumen&idioma=SPA>.
- Martínez Otero, Juan Maria; "La Difusión de Sexting Sin Consentimiento Del Protagonista: Un Análisis Jurídico," no. 12 (2013): 1–16.
- Menjívar Ochoa, Mauricio. "EL SEXTING Y L @ S NATIV @ S NEO-TECNOLÓGIC @ S : APUNTES PARA UNA CONTEXTUALIZACIÓN AL INICIO DEL SIGLO SEXTING AND NEO-TECHNOLOGICAL NATIVES : Mauricio Menjívar Ochoa EL SEXTING Y L @ S NATIV @ S NEO-TECNOLÓGIC @ S : Mauricio Menjívar Ochoa 1." *Revista Electrónica Publicada Por El Instituto de Investigación En Educación Universidad de Costa Rica* 10, no. 1409–4703 (2010): 24.
- Mnisterio del Interior (gabinete de Coordinación y Estudios). "Anuario Estadístico de Ministerio Interior." *BOE* 53, no. 9 (2013): 15. doi:10.1017/CBO9781107415324.004.
- Pérez, Pablo, Susana De la Fuente, Laura García, Jesús Guijarro, and María De Blas. "Estudio Sobre La Seguridad Y Privacidad En El Uso de Los Servicios Móviles Por Los Menores Españoles." *Inteco*, 2010, 153.
- Quintero Olivares, Gonzalo. *Comentario a La Reforma Penal de 2015*. Cizur Menor, Navarra : Thomson Reuters Aranzadi, 2015. http://cataleg.urv.cat/record=b1496194~S13*cat.
- . "Internet y derecho penal: imputación de los delitos y determinación de la competencia." *La ley penal: revista de derecho penal, procesal y penitenciario*.

- Wolters Kluwer, 2007. <https://dialnet.unirioja.es/servlet/articulo?codigo=2259130>.
- Tascón, María Marta González. “El Nuevo Delito de Acceso a Niños Con Fines Sexuales a Través de Las TIC.” *Estudios Penales Y Criminológicos XXXI*, no. 31 (2011): 207–58.
- Torres Alberro, Cristóbal (Dir.), José Manuel Robles, and Stefano De Marco. “El Ciberacoso Como Forma de Ejercer La Violencia de Género En La Juventud: Un Riesgo En La Sociedad de La Información Y Del Conocimiento,” 2013, 165. doi:NIPO: 680-13-092-1.
- Toste, Y A N Vera. *Autoría Y Participación*. UNIJURIS,, 2015. <http://www.lex.uh.cu/sites/default/files/6>. VERA, Yan - Autoría y Participación.pdf.
- Velasco Núñez, Eloy. *Delitos Cometidos a Través de Internet : Cuestiones Procesales*. Las Rozas (Madrid) : La Ley, 2010. http://cataleg.urv.cat/record=b1406593~S13*cat.

LEGISLACIÓN

Cortes Generales. “Ley 34 / 2002 , de 11 de Julio , de Servicios de La Sociedad de La Información Y de Comercio Electrónico . TEXTO CONSOLIDADO Última Modificación : 10 de Mayo de 2014,” 2014, 1–32.
<https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>.

Ue, Directiva, D E L Parlamento, and Europeo Y Del. “Directiva 2011/93/UE, Relativa a La Lucha Contra Abusos Sexuales Y La Explotación Infantil,” 2011, 1–14.

“Ley Orgánica 10/1995, de 23 de Noviembre, Del Código Penal. TÍTULO XIII. Delitos Contra El Patrimonio Y Contra El Orden Socioeconómico.,” n.d.

“Constitución Española, 1978.,” accessed March 7, 2016,
http://noticias.juridicas.com/base_datos/Admin/constitucion.html.

JURISPRUDÈNCIA

- Auto de procedimiento abreviado 0001109 /2012, del Juzgado de Instrucción nº 1 de Orgaz (Toledo) en fecha 15 de marzo de 2013.
http://www.encastillalamancha.es/archive/files/20130422134247_EOGQXG.pdf

- Sentencia de la Audiencia Provincial de Huelva, de 15 de febrero de 2002 (SAP H 178/2002) *CENDOJ*
<http://www.poderjudicial.es/search/indexAN.jsp>

- Sentencia de la Audiencia Provincial de Alicante de 02 de febrero de 2012 (SAP A 1331/2012) *CENDOJ*
<http://www.poderjudicial.es/search/indexAN.jsp>

- Sentencia del Tribunal Supremo núm 2222/2013 de 17 de Abril de 2013, (RTC 1461/20012) *CENDOJ*
http://190.104.117.163/2014/septiembre/Proteccion_a_menores/contenido/ponencias/Anexos/Jurisprudencia/STS%202013.Registro%20de%20ordenadores.pdf

- Sentencia Tribunal Constitucional núm 14/2003 (Sala Segunda) de 28 de enero. (RTC 2003\14) *BOE*,34.
<http://doi.org/10.1017/CBO9781107415324.004>

WEBGRAFIA

- Mossos d'Esquadra de la Generalitat de Catalunya. (2015) *Formulari de contacte*. Recuperado 14/04/2016 desde <https://ovt.gencat.cat/gsitfc/AppJava/generic/conqxsGeneric.do?webFormId=351>
- Generalitat de Catalunya. (2015) *Real Decret 415/2011*. Recuperado 06/04/2016 desde http://dogc.gencat.cat/ca/pdogc_canals_interns/pdogc_resultats_fitxa/?documentId=594021&language=ca_ES&action=fitxa
- Fiscales del Estado Español. (2015) *Memorias de la Fiscalía*. Recuperado 10/04/2016 desde https://www.fiscal.es/fiscal/publico/ciudadano/documentos/memorias_fiscalia_general_estado/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOI9HT0cDT2DDbwsgozNDBwtjNycnDx8jAwszPQLsh0VAQluD0w!/?selAnio=2012
- Pantallas amigas (2015). *Sextorsión, prácticas arriesgadas y fallos de seguridad al servicio del delito*. Recuperado 03/05/2016 desde <http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/sextorsion-practicas-arriesgadas-y-fallos-de-seguridad-al-servicio-del-delito.shtml>
- Ernest Codina (2016) *El «sextorsion» et podria arruïnar la vida. Saps què és?* Nació Digital. Recuperado 20/03/2016 de : <http://www.naciodigital.cat/noticia/104856/sextorsion/et/podria/arruinar/vida/saps>