Universidad de Valladolid

Facultad de Derecho

Grado en Criminología

"Análisis y Soluciones para la prevención de la violencia ejercida a través de las TIC en jóvenes y niños"

Presentado por:

D. Luis Ojeda Martínez

Tutelado por:

Dra. Dª. Beatriz Sainz de Abajo

Valladolid, junio de 2018

Universidad de Valladolid

CONVOCATORIA: JUNIO 2018

TITULO:

"Análisis y Soluciones para la prevención de la violencia ejercida a través de las TIC en jóvenes y niños"

AUTOR: D. Luis Ojeda Martínez

TUTORA: Dra. Dª. Beatriz Sainz de Abajo

COMISIÓN EVALUADORA:

PRESIDENTE: Dra. Dª. Beatriz Sainz de Abajo

VOCAL 1: Dr. D. Miguel López-Coronado Sánchez-Fortún

VOCAL 2: Dra. Dª. Isabel de la Torre Díez

SUPLENTE 1º: Dr. D. Carlos Gómez Peña

SUPLENTE 2º: Dr. D. Jesús Poza Crespo

SUPLENTE 3ª: Dra. Dª. María García Gadañón

RESUMEN:

La accesibilidad a las Tecnologías de la Información y la Comunicación ha generado una nueva forma de acceder a la información y de establecer relaciones entre las personas.

Este trabajo presenta la necesidad de prevenir situaciones de riesgos. Hay que prestar atención a la seguridad en el uso de Internet y las TIC por parte de las personas menores de edad. El objetivo del documento es analizar la respuesta del ordenamiento penal español a las distintas formas de acoso sexual, y/o no sexual, a menores realizado en el ciberespacio.

ABSTRACT:

Accessibility to Information and Communication Technologies has generated a new way of accessing information and establishing relationships between people.

This work presents the need to prevent risk situations. Attention must be paid to security in the use of the Internet and ICTs by minors. The objective of the document is to analyze the response of the Spanish penal code to the different forms of sexual molestation, and / or non-sexual, to minors carried out in cyberspace.

PALABRAS CLAVE:

TIC, menores, redes sociales, cibercrimen social, conductas de riesgo, prevención.

KEY WORDS:

ITC, minors, social networks, social cybercrime, risk behaviors, prevention.

AGRADECIMIENTOS:

Como de bien nacido es ser agradecido, quiero expresar aquí mi enorme gratitud a mis padres, a mi hermana, a mi esposa y a mis dos hijas por su apoyo incondicional en este reto personal propuesto.

Igualmente, agradecerle a la tutora de este trabajo por su apoyo y orientación, destacando su calidad personal y profesional. Gracias, Dª. Beatriz Sainz.

TABLA DE CONTENIDO

LISTADO DE IMAGENES

1. INTRODUCCIÓN.

En los últimos años el desarrollo de las nuevas tecnologías ha propiciado nuevos espacios de socialización. Esta era digital en la que actualmente jóvenes y personas adultas se encuentran inmersas, ha supuesto una interrupción en los patrones de relación tradicionales. Mientras que la infancia y la adolescencia crecen en entornos digitales, usando *tablets*, *smartphones*, libros electrónicos y ordenadores personales de forma intuitiva, jugando online, conociendo a terceros/as a través de perfiles digitales y encontrando respuestas a sus dudas en la red, las personas adultas incorporan una nueva forma de relación añadida a la que ya conocían, y por consiguiente, opcional. Esta diferencia entre crecer interiorizando el entorno virtual como forma imprescindible de socialización y hacerlo como ingrediente añadido es lo que determina el concepto de "brecha digital". Según Marc Prensky[1], los conceptos que mejor definen a ambos grupos serían "nativos digitales" e "inmigrantes digitales". Los *nativos digitales* serían quienes han nacido y se han formado usando la particular "lengua digital" de juegos por ordenador, vídeo e Internet. Por su parte, los *inmigrantes digitales* serían aquellas personas que no han vivido intensamente esta era, pero se han visto obligadas a sumergirse con celeridad en el uso de las nuevas tecnologías.

Según los datos del Instituto Nacional de Estadística (2015) más del 85% de los jóvenes hace uso de Internet a partir de los 10 años, alcanzado el 99% cuando sobrepasan los 15 años. Se trata de un sector de la población que ha crecido rodeado de tecnología y que, por ello, domina el lenguaje digital.

La socialización digital tiene una serie de características que la distinguen de las formas tradicionales de interacción interpersonal. La primera y más significativa de ellas es el acceso directo y constante a las redes sociales, el llamado "efecto 24 x 7" (veinticuatro horas y siete días a la semana). A través de ellas ya no es necesario coincidir en un mismo espacio físico, ni siquiera en el mismo momento. Las nuevas tecnologías favorecen una comunicación atemporal. Esto viene a decir, que la persona emisora puede dirigirse cuando

[1] PRENSKY, M. (2001), *"Digital Natives, Digital Immigrants"*. In on the horizon, October 2001, 9 (5) NCB University Press.

lo prefiera a otras sin necesidad de coincidir con ella en el tiempo, por ejemplo a través de los muros y tablones de las redes sociales. Esta opción ha supuesto un medio para agilizar la inmediatez de la comunicación en esta sociedad 2.0 que, por otra parte, provoca un "efecto eco". Toda aquella información que se sube a Internet, es susceptible de difundirse perdiendo el control la persona emisora de dónde y quienes acabarán accediendo a la misma.

Por otra parte, las relaciones a través de las redes sociales tienen una serie de repercusiones en el modo de interactuar tanto jóvenes como personas adultas. Al margen de las positivas, entre las que se encuentran el acceso a la información, la posibilidad de contactar fácilmente con personas conocidas y desconocidas y/o disponer de un banco de recursos y de opciones de ocio ilimitado, se encuentran otras que pueden ocasionar dificultades en las relaciones entre iguales.

Relacionarse a través de las nuevas tecnologías favorece una falsa sensación de anonimato, por el hecho de desarrollarse desde espacios privados y terminales propios cuya repercusión se sitúa en el mundo virtual, y propiciando una dificultad para empatizar con quienes se interactúa debido a que no se dispone del reflejo emocional de quienes están al otro lado de la red. El hecho de no disponer de la información visual, la comunicación verbal y no verbal y la reacción que provoca en otras personas las intervenciones que se plasman en las redes sociales, aventura en ocasiones a jóvenes y adolescentes a ser más osados en sus comentarios.

Derivado de lo anterior, se produce una dificultad para concebir que los actos que tienen lugar en el mundo virtual tengan consecuencias en el mundo real. Así mismo, es habitual encontrar una concepción de privacidad distinta en función del mundo en el que se interactúe. Esto es, que si bien algunas conductas se asumen que no se realizarían en el mundo "offline" por pertenecer al ámbito privado (pasearse por la calle en ropa interior), sí se contempla llevarlas a cabo en el mundo "online" por no ser conscientes de las repercusiones que sí que tienen también en este ámbito (subir una foto en ropa interior a una red social con perfil público).

La violencia ejercida a través de las redes sociales digitales no descubre técnicas ni conceptos diferentes de violentar a otras personas de los que tradicionalmente se han

identificado. Lo que sí ofrece la Web 2.0 es un nuevo escenario en el que se producen formas de victimización.[2]

La escasez de material bibliográfico y estudios específicos sobre las consecuencias psicológicas derivadas de la victimización sufrida a través de las redes sociales digitales, impide desarrollar intervenciones profesionales de mayor calidad y ajustadas a las necesidades de las víctimas. Ni que decir tiene que, consecuentemente, las victimas no reciben la asistencia ajustada a su demanda real.

Dado lo anterior, se detecta la necesidad imperiosa de dotar a profesionales de estrategias de prevención que favorezcan la generalización en la ciudadanía de un uso adecuado de las redes sociales. Así como, a nivel de atención e intervención, es también imprescindible que se les dote de criterios y herramientas específicas.

La ya mencionada "brecha digital" ha dificultado no sólo el que desde ámbitos profesionales no se haya identificado el espacio virtual como un lugar de victimización más, sino que además ha impedido a padres y madres educar virtualmente a sus hijos e hijas.

El hecho de tratarse de "inmigrantes digitales" coloca a las personas adultas, y referentes educativos de menores y jóvenes, en una situación de vulnerabilidad. Dado que para "inmigrantes digitales", Internet es un elemento añadido a su cotidianeidad, les resulta complicado asumir que para "nativos digitales", Internet sea un espacio de relación imprescindible. Por todo ello, el modelo que generalmente se practica entre educadores/as y progenitores/as suele ser un modelo represivo, donde las opciones que se facilitan para prevenir riesgos y afrontar situaciones conflictivas virtuales van dirigidas a la restricción del uso de las redes sociales digitales, así como a limitar las acciones que en ellas se desarrollan (subir fotos, participar en grupos, actualizar estados, compartir información, etc.). Este modelo represivo aleja a los/as garantes de la protección de la infancia y adolescencia de las

[2] MIRÓ, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio.
Revista Española de Investigación Criminológica Artículo 5, Número 11 (2013)
www.criminologia.net

necesidades reales de éstas. La peor consecuencia de este modelo es que ese miedo a no tener acceso a Internet, favorece la ley del silencio (que menores y jóvenes no compartan en casa o con adultos situaciones problemáticas vividas en Internet) y que busquen soluciones entre sus iguales. El ser "nativo digital" conlleva una falsa sensación de experto, es decir, se manejan intuitivamente con las nuevas tecnologías, pero carecen de estrategias para afrontar determinadas situaciones. Por tanto, en el caso de ser agredidos virtualmente, este modelo podría potenciar la victimización secundaria, agravando las consecuencias psicológicas derivadas de la acción delictiva inicial (ciberacoso, sextorsión*, ciberbullying*, etc.).

2. DEFINICIÓN DEL CIBERACOSO.

El ciberacoso se puede definir como la acción de llevar a cabo "*amenazas, hostigamiento, humillación u otro tipo de molestias realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, correo electrónico, mensajería instantánea, videoconsolas online, etc.*"[3]

El ciberacoso, por lo tanto, se convierte en una situación aún más grave cuando estamos hablando de la implicación de menores o de adultos y menores.

2.1. Principales conductas dentro del acoso a menores.

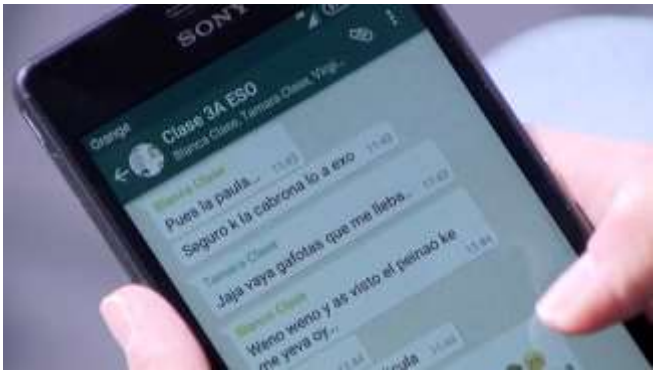
2.1.1. Ciberbullying.

De este fenómeno se pueden obtener múltiples definiciones, pero en general, se puede determinar como una conducta de acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

En una definición más exhaustiva, se puede decir que el *ciberbullying* supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de los medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la

[3] Definición extraída de Aftab, Parry, Guía práctica sobre el ciberbullying, adaptada y contextualizada por Jorge Flores y Manu Casal de Pantallas Amigas.

mensajería de texto a través de dispositivos móviles o la publicación de vídeos o fotografías en plataformas electrónicas de difusión de contenidos. Por tanto, se trata del uso de los canales telemáticos de comunicación que ofrecen las TIC para realizar un acoso psicológico hostil y reiterado por parte de un menor o grupo de menores a otro menor.



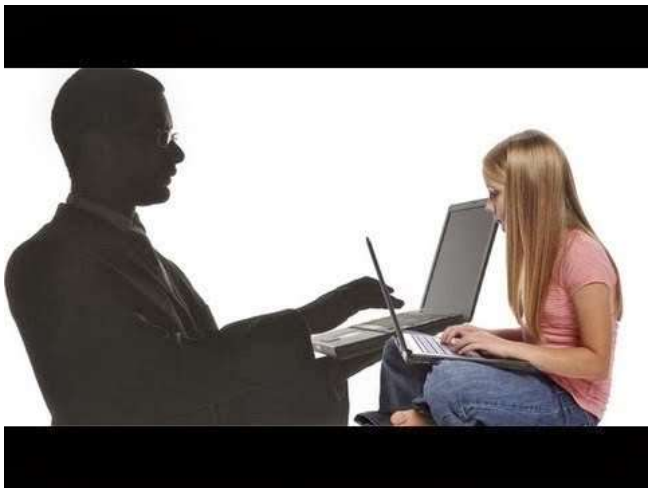
[4]**Imagen 1.-** Acoso a menores a través del *cyberbullying*

2.1.2. Child grooming, grooming o ciberacoso con intención sexual.

El *grooming*, por su parte, se define como un acoso ejercido por un adulto y se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor. Se podría decir que son situaciones de acoso con un contenido sexual explícito o implícito.

Por tanto, se trata de aquellas acciones preconcebidas que lleva a cabo un adulto a través de Internet para ganarse la confianza de un menor de edad y obtener su propia satisfacción sexual mediante imágenes eróticas o pornográficas que consigue del menor, pudiendo llegar incluso a concertar un encuentro físico y abusar sexualmente de él.

[4] https://www.youtube.com/watch?v=bfUDw-0IHFk



[5]**Imagen 2.-** Acoso a menores a través del *grooming*

2.1.3. Ciberstalking.

El *ciberstalking* es, básicamente, acoso online. Se ha definido como el uso de tecnología, en particular Internet, para acosar a una persona. Algunas de las características comunes son: acusaciones falsas, seguimiento, amenazas, robo de identidad y destrucción o manipulación de datos.

[6]**Imagen 3.-** Acoso a menores a través del *cyberstalking*

[5]https://www.elancasti.com.ar/policiales/2017/7/10/cada-argentinos-saben-grooming-340645.html

[6] https://dailypost.in/ludhiana/b-tech-dropout-held-cyber-stalking/

2.1.4. Sexting.

Sexting es una palabra tomada del inglés que une "*Sex*" (sexo) y "*Texting*" (envío de mensajes de texto vía SMS desde teléfonos móviles). Aunque el sentido original se limitase al envío de textos, el desarrollo de los teléfonos móviles ha llevado a que actualmente este término se aplique al envío, especialmente a través del teléfono móvil, de fotografías y vídeos con contenido de cierto nivel sexual, tomadas o grabados por el protagonista de los mismos.

La conducta lesiva se materializa cuando el receptor del material audiovisual –generalmente remitido de manera voluntaria por su protagonista, aunque muchas veces también "robada" mediante intrusión informática- pasa a manos de terceras personas y circula de manera libre y generalizada entre una infinidad de ellas a través de cualquiera de los canales de las TIC (teléfonos móviles, redes sociales, e incluso el sitio web YouTube), provocando en la victima –el propio menor que ha producido la imagen- un grave daño moral y psicológico que, en muchas ocasiones, deriva en *ciberbullying* porque esas imágenes son utilizadas para denostarla y humillarla.

Otra forma de utilización maliciosa de este tipo de imágenes, previa a la difusión, se realiza mediante la coacción o la amenaza de dicha difusión para obtener un beneficio, que puede ir desde lo simplemente material, hasta la denigración de la víctima o la obtención de favores sexuales, lo cual implica una doble victimización y supone un grado añadido de daño psicológico y moral, con graves implicaciones penales.

Relacionado con el *sexting* se encuentra el llamado "*sex-casting*". Con este término se identifica la grabación de contenidos sexuales a través de la webcam y difusión de los mismos por e-mail, redes sociales o cualquier canal que permitan las nuevas tecnologías.

[7]**Imagen 4.-** Acoso a menores a través del *sexting*

2.1.5. Sextorsión.

Este neologismo tiene su origen en el inglés *sextortion* que es una forma de explotación sexual en la cual se chantajea a una persona por medio de una imagen de sí misma desnuda que ha compartido a través de Internet mediante *sexting*.

La víctima es posteriormente coaccionada para tener relaciones sexuales con el/la chantajista, para producir pornografía u otras acciones. El chantaje se suele realizar por Internet, ya que asegura un cierto grado de anonimato al criminal.

La sextorsión puede ser a menores de edad o a adultos. Por medio de imágenes obtenidas mediante webcam, email, mensajería instantánea, teléfonos u otros dispositivos móviles; es decir, por todos los medios que sirven para realizar *sexting*. Con objeto de un abuso sexual, una explotación pornográfica para uso privado, para redes pedófilas o comercial, una extorsión económica o cualquier otro tipo de coacción puntual o continuada. Realizada por conocidos, ex-amantes o personas desconocidas.

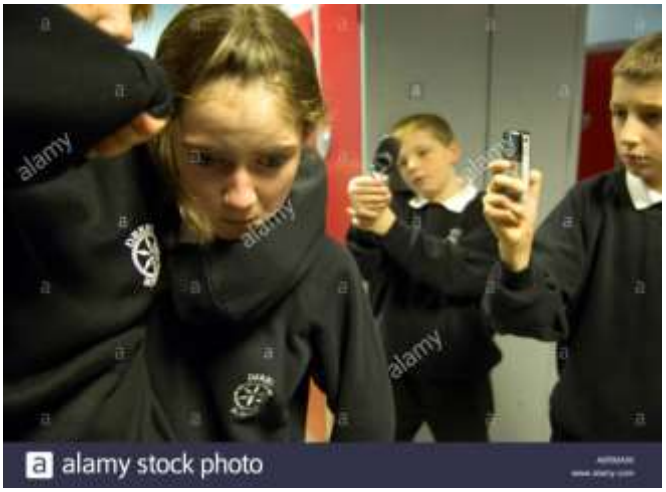
[7]http://www.e-consulta.com/nota/2017-10-25/entretenimiento/el-sexting-es-comun-en-sociedades-de-doble-moral-dice-academica

[8]**Imagen 5.-** Acoso a menores a través de la sextorsión

2.1.6. Happy slapping ("bofetada feliz").

Se trata de una acción, generalmente colectiva, en la que un grupo de menores agrede a otro menor para humillarlo –la forma más usual se realiza por medio de una fuerte e inesperada bofetada- como parte de una especie de juego o reto, la cual es grabada con algún medio tecnológico (normalmente un teléfono móvil) y difundida posteriormente a través de las TIC.

La acción puede tener su continuidad y derivar en *ciberbullying* por el componente de humillación de la misma.



[9]**Imagen 6.-** Acoso a menores a través del *happy slapping*

[8] http://www.codigonuevo.com/sociedad/sextorsion-alguien-chantajea-publicar-fotos-intimas

[9]http://www.alamy.com/stock-photo-happy-slapping-bullying-mobile-phones-cameraphones-video-record-school-11638272.html

2.2. Acoso cometido por menores: Ciberbaiting o arbaiting.

Esta conducta es una modalidad de acoso en la que el agresor es un menor o grupo de menores y la víctima un docente, realizándose mediante un mecanismo similar a como se da el *ciberbullying*, mediante el hostigamiento psicológico reiterado y con el ánimo de humillar y denigrar al profesor, muchas veces como continuidad a actitudes similares que tienen lugar en el aula o el centro escolar.

Esta nueva forma de acoso a los docentes tiene su origen en acciones de humillación pública en el ámbito "real" del centro escolar o en agresiones físicas a su persona o bienes, y puede ocasionar graves perjuicios psicológicos y morales a la víctima que acaben por afectar a su motivación, generado apatía, o, en los casos más graves y persistentes, la baja por razones psicológicas.

[10]**Imagen 7.-** Acoso cometido por menores a través del *ciberbaiting*

2.3. Elementos empleados en el acoso a través de medios tecnológicos.

Los principales medios tecnológicos a través de los cuales los menores reciben, y pueden llevar a cabo, actos de acoso, son los siguientes:

- Medios de contacto electrónico.

[10] https://computerhoy.com/noticias/internet/mi-hijo-practica-ciberbaiting-que-hago-12485

Programas de mensajería instantánea, chats públicos, foros de discusión y correo electrónico.

Son herramientas que favorecen y facilitan las comunicaciones entre los menores, pero al mismo tiempo constituyen un nuevo canal a través del cual se pueden recibir contenidos y mensajes susceptibles de constituir acoso.

En este sentido, cabe señalar la conducta de vejaciones realizadas a través de correo electrónico, en la que se utiliza este servicio electrónico para proferir amenazas e insultos. Ante esta situación puede investigarse la cuenta desde la que se envían los mensajes, pero resulta más compleja la identificación del usuario que efectivamente es autor de los mismos.

- Teléfonos móviles multimedia.

La aparición y difusión de teléfonos móviles con cámara de fotos y video constituye un canal que, en manos de usuarios acosadores, supone un nuevo medio con el que realizar actos de intimidación.

El hecho de contar con un dispositivo móvil capaz de captar imágenes en formato digital y remitirlas inmediatamente a todos los contactos hace que cualquier imagen lesiva contra un menor se pueda difundir técnicamente de forma inmediata entre un gran número de personas.

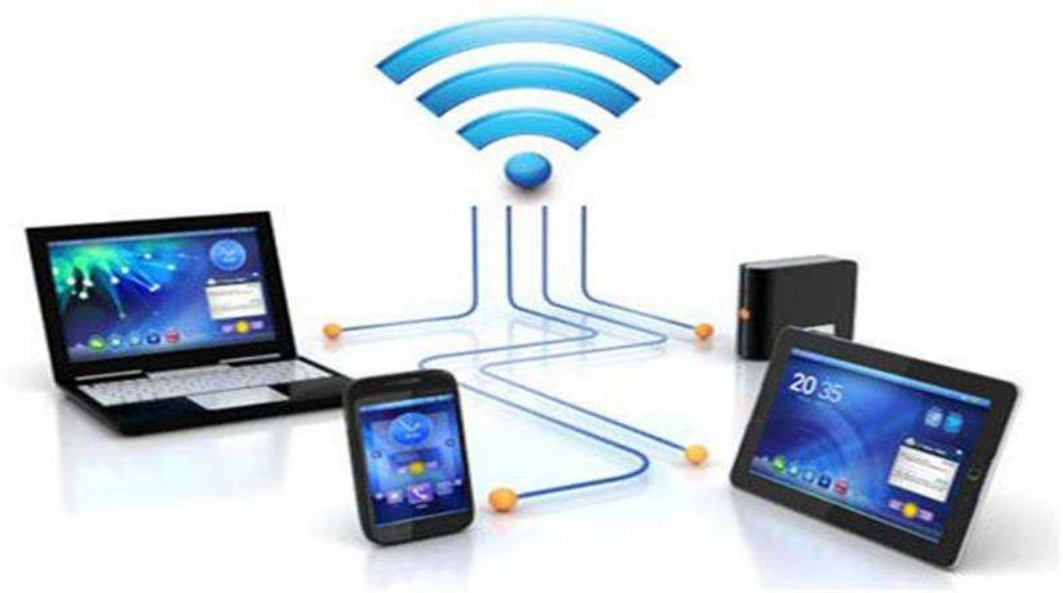
- Uso de plataformas online de difusión de contenidos.

Un gran número de casos de acoso online se convierten en situaciones de riesgo más grave para los menores, en la medida en que el medio empleado para la difusión de información vejatoria o difamatoria lo constituyen las plataformas online de difusión de contenidos que permiten la publicación de vídeos o imágenes fijas y el visionado por millones de personas de todo el mundo.

Así, lo que en principio nace como una mera fotografía o vídeo alojados en un dispositivo móvil pasa a ser difundido de forma masiva y mundial, logrando que el efecto dañino buscado por el acosador conlleve un mayor impacto.

- Uso de redes sociales.

Con frecuencia, los menores emplean las redes sociales con medio para intercambiar impresiones y comunicarse con sus compañeros.



[11]**Imagen 8.-** Principales medios tecnológicos empleados en el ciberacoso

El alto grado de difusión y viralidad[12] de las redes sociales, y la posibilidad de publicación de fotografías y vídeos por parte de sus miembros, hacen que este tipo de plataformas resulte un nuevo medio especialmente atractivo para los acosadores.

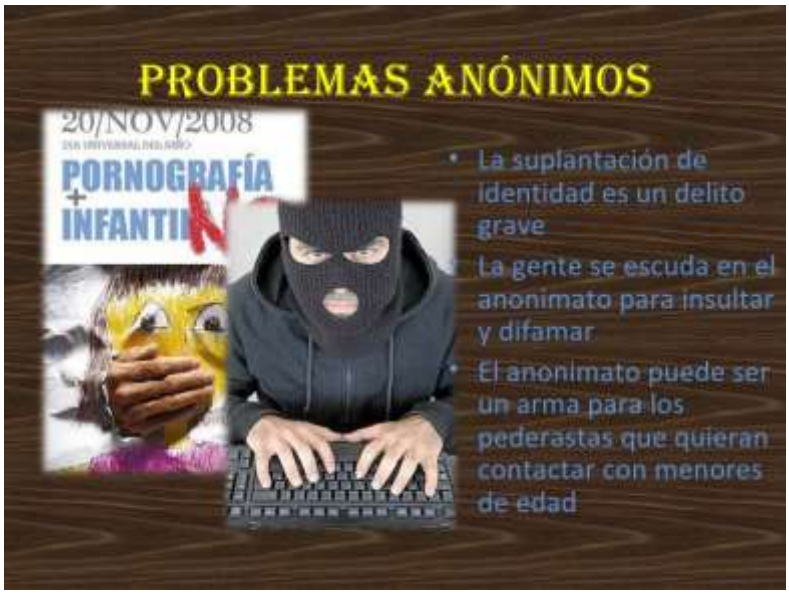
[11]https://techviral.net/wp-content/uploads/2015/08/Selected-Device-To-Connect-To-Your-Wifi-830x450.jpg

[12] Cuando se habla de viralidad respecto a las redes sociales, se hace referencia a la capacidad que tienen este tipo de redes para lograr el máximo crecimiento en número de usuarios, en el menor tiempo posible.

2.4. ¿Cuál es la razón del empleo de las TIC para estas conductas?

El principal elemento que debe tenerse en cuenta es la sensación de anonimato que otorga Internet a los usuarios. En este sentido, es necesario destacar que existen medios tecnológicos suficientes para poder determinar el lugar exacto y el equipo informático desde el que se llevó a cabo el presunto delito.

Así, menores de edad, padres y tutores deben ser informados de que siempre que navegan a través de Internet, lo hacen a través de una dirección IP que su proveedor de Internet facilita. Esta dirección IP funciona como una especie de "matrícula" en la Red, que permite la identificación de los equipos de los usuarios y conocer a quién pertenece la conexión de Internet. Este dato, que únicamente puede ser conocido y utilizado previa solicitud judicial, es clave para poder perseguir a los autores de las actividades de acoso. Junto a la dirección IP, con frecuencia las investigaciones llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado (en adelante FCSE) emplean servicios públicos de Internet, como redes sociales, buscadores de Internet, programas de mensajería instantánea, etc, para averiguar la identidad de los presuntos acosadores.



[13]**Imagen 9.-** Razón del empleo de las TIC para realizar el ciberacoso

[13]https://image.slidesharecdn.com/elanonimatoenlared-090301102600-phpapp02/95/el-anonimato-en-la-red-ppt-5-728.jpg?cb=1235903197

3. ANÁLISIS JURÍDICO DEL ACOSO A MENORES.

3.1. Perfil del delincuente informático.

En la actualidad es la delincuencia del presente, del ahora mismo, en la que, como en todas, cada caso es un aparte, pero especialmente dada a la confección de patrones de conducta y pautas que, por obra de la estadística, nos permiten emitir el perfil del atacante tipo o estándar, que responde principalmente, a los siguientes parámetros:

- Sus autores, normalmente son personas en la decena de los 40 o menos años de edad, especialmente gente muy joven, nativos digitales o casi, más habituados a teclear que a grafiar, y que en consecuencia, a la hora de delinquir usan el medio de expresión con el que están más familiarizados, aquel, precisamente, con el que otros más mayores no lo están, formando el grupo de sus víctimas más comunes, junto con los menores de edad y desvalidos.

- Aunque al principio tuvo mucho predicamento la figura del delincuente travieso y solitario que nos enseñaba que cualquier sistema informático es de por sí inseguro y penetrable, con el transcurso del tiempo, en la actualidad, el delincuente informático más habitual es el que busca en grupo criminal organizado amenazas permanentes avanzadas.

- Y aunque es cierto que el grupo más numeroso de autores delictivos son personas que no sabiendo informática ni aun programar, son buenos en aquello a lo que dedican muchas horas, esto es navegar y usar la informática, llama poderosamente la atención que, como en pocas, en este tipo de acciones delictivas se vaya deteniendo no ya solo a gente nada desestructurada socialmente hablando, sino incluso a gente con carrera universitaria, que no suelen ser profesionales implicados de manera numerosa en ningún otro tipo de delitos.

3.2. Tipos penales.

Antes de empezar el análisis de la descripción de los tipos delictivos, conviene hacer una reflexión de la mezcla que supone derecho penal y menores.

El Derecho Penal, en la tarea de evitación de las conductas violentas en el contexto educativo, constituye el último recurso en manos del Estado, dada la exigencia, inexcusable en un Estado Social y Democrático de Derecho, de respetar el principio de última ratio y prohibición de exceso en la estructuración de los sistemas de tutela de los proyectos vitales de los menores.

En nuestro ordenamiento jurídico, el artículo 19 del Código Penal[14] estipula las líneas maestras del modelo regulador de la responsabilidad de los menores de dieciocho años que cometan un hecho tipificado como infracción penal. Dispone que estos menores no serán responsables criminalmente con arreglo a la regulación contenida en el Código Penal, estipulando que cuando un menor de dicha edad cometa un hecho delictivo podrá ser responsable con arreglo a lo dispuesto en la ley que regule la responsabilidad penal del menor[15] (en adelante LORPM). Desarrollando esta previsión, se promulga la LO 5/2000, que fue modificada por la LO 7/2000 y la LO 8/2006 y desarrollada por el RD 1774/2004.

Conviene tener presente que estos tipos de conductas ilícitas resultan de difícil investigación para el Juez Instructor o Fiscal, y al mismo tiempo representan mayor gravedad y llevan implícita una mayor facilidad de difusión, así como un mayor impacto en la víctima y una falta de empatía por parte del autor.

Sobre la temática que nos ocupa, tenemos que referenciar también la Ley de Protección de Datos de Carácter Personal[16] (en adelante LOPD) artículos 5 y 6, y el RD 1720/2007, de 21 de diciembre, de desarrollo de esta ley donde, en su artículo 13.1, se regula la captación de datos personales de los menores de edad y su uso.

[14] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[15] Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores.

[16] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Así, se establece que se podrá proceder al tratamiento de datos de los mayores de 14 años con su consentimiento, salvo aquellos casos en que la ley exija para su prestación la existencia de autorización de los titulares de la patria potestad o tutela. En el caso de los menores de 14 años, se requerirá el consentimiento de los padres o tutores.

Esta circunstancia resulta extrapolable a casi todas las redes sociales, aparezca o no en sus condiciones de uso.

La LOPD regula, entre otras cosas, el uso que se hace de los datos personales, imágenes o vídeos de terceros y regula la sanción en el caso de que se atente contra la intimidad y privacidad de las personas.

Los especialistas en la jurisdicción de menores recomiendan la regulación de las responsabilidades civiles que de ello se deriven recurriendo a las recomendaciones legales que plantean los Tratados Internacionales al respecto en relación a la prevención y a la persecución de las conductas delictivas relacionadas con Internet.

El ciberacoso está integrado por una pluralidad de hechos que pueden encontrar acomodo en los tipos penales que tratan de proteger los intereses personalísimos de la persona. Podría tratarse de delitos como amenazas, coacciones, integridad moral, agresiones y abusos sexuales, calumnias e injurias, etc.

3.2.1. Amenazas.

Se encuentran reguladas en los **artículos 169 a 171** del Código Penal, donde se dispone que la comisión de este tipo de delitos requiere del cumplimiento de los siguientes elementos:

- Que exista una amenaza.
- Que la amenaza consista en causar un mal (sea delito o no).
- Que exista una condición para no causar dicho mal.

En la mayor parte de los casos, las amenazas constituyen la situación de acoso vivida por la víctima en la vida física (centros escolares, normalmente), encontrándose indefenso el menor ante el ataque reiterado por parte del acosador.

El mal con el que se amenaza a la víctima puede ser constitutivo de delito o no, pero debe destacarse como la amenaza más empleada en Internet se encuentra directamente relacionada con el honor y la intimidad del afectado (*ciberbullying*), existiendo casos en los que el coaccionador intimida a su víctima con la publicación de imágenes o vídeos que pueden situarlo en una posición comprometida respecto a terceros.

Con frecuencia esta situación es ocultada por parte del menor afectado, a pesar de contar con la regulación y protección jurídica específica, por temor a las represalias que pudieran derivarse.

3.2.2. Coacciones.

Se encuentran reguladas en los **artículos 172 y 173** del Código Penal, donde se dispone que la comisión de este delito requiere del cumplimiento de los siguientes elementos:

- Que se obligue a un tercero a hacer o dejar de hacer algo.
- Que dicha obligación se lleve a cabo mediando violencia.

Concretamente, en el **artículo 172 ter** del Código Penal se pena una especie de acoso (*stalking*), a caballo entre la coacción y la amenaza que no es propiamente ni una ni otra –y si acaso concurre, se pena por concurso real ex art. 172 ter 3º CP-, en la que se consiga alterar gravemente el desarrollo de la vida cotidiana de la víctima –resultado que debe probarse, principalmente mediante pericia psicológica, que no concurre ante ciertas personalidades fuertes indiferentes-, cuando de forma insistente y reiterada –descartando casos puntuales- y sin estar legítimamente autorizado:

- Someta a vigilancias, persecuciones o busque su cercanía física.

- Contacte o intente contactar por cualquier medio de comunicación –llamadas jadeantes, llamadas que inmediatamente cuelgan o no hablan, o llamadas muy constantes- o mediante tercera persona –si hay orden de alejamiento comunicativo, por principio de especialidad, es aplicable el artículo 468 CP-.
- Use indebidamente sus datos, contratando mercancías/servicios o haciendo que terceras personas se pongan en contacto con ella –en una especie de suplantación que muchas veces se hará tecnológicamente- o
- Atente contra su libertad o patrimonio –rallándole el coche, por ejemplo-, o los de persona próxima a ella.

El delito afecta a la libertad de obrar –normalmente determinando a conductas diferentes a las deseadas- y al sentimiento de seguridad, a través de esa atmosfera de presión que busca el derrumbe moral que puede llevar a deterioros psíquicos en la victima que pueden incluso acabar en el suicidio.

Exige con la "insistencia y reiteración", la exteriorización de más de un acto –de la misma o distinta naturaleza de los descritos en el tipo- y debe quedar probado que el hostigamiento de ese patrón de conducta, va dirigido a una víctima precisa con el resultado objetivo de generar la inquietud o desasosiego que afecte psíquicamente.

3.2.3. Abuso sexual.

En el **artículo 183 bis** del Código Penal se castiga como abuso a quien con fines sexuales –cuyo propósito debe constar acreditado- determine –esto es, sea causante- a un menor de 16 años a participar en un comportamiento de naturaleza sexual, o le haga presenciar actos de esa naturaleza, aunque el autor no partícipe en ellos; lo que convierte el hacer ver películas o escenas sexuales en cualquier tipo de soporte tecnológico a un menor de 16 años en un abusador –por la corrupción que se consigue sobre el menor-, tipificando uno de los escasos delitos del Código Penal que se cometen a través de la vista.

Si lo presenciado es un abuso sexual –y no cualquier otro delito sexual como la pornografía sexual infantil-, la norma impone lógicamente pena mayor.

El tipo penal más próximo en el caso del *grooming* está en el **artículo 183 ter** del Código Penal al comprender dos modalidades que combinan la acción virtual tecnológica con una posterior exteriorización de la conducta que pena el abuso de confianza, la explotación de la ingenuidad de los menores, la captación de pornografía infantil y el intento de abuso sexual, que plantea difíciles problemas concursales:

- Contactar por Internet, por teléfono o por cualquier otra TIC con un menor de 16 años para propiciar un encuentro para intentar en él, bien cualquier delito de abuso sexual, bien de pornografía infantil –parte de la acción que se realiza a través de las TIC en el llamado mundo virtual- más además actos materiales –ya en el mundo físico- encaminados al acercamiento.

  Si únicamente se da la conducta en el mundo tecnológico sin siquiera acercamiento, puede pensarse en formas imperfectas de ejecución.

  Si se consuman los delitos pretendidos de los artículos 183 o 189 del CP, se penan en concurso real, y si el acercamiento se consigue mediante coacción, intimidación o engaño, reciben mayor pena.

- Contactar mediante las TIC con un menor de 16 años –en el mundo virtual-, más además realizar actos dirigidos a embaucarle para (*sexting*) que:
  - Facilite material pornográfico –propio o ajeno-, o
  - Muestre imágenes pornográficas –propias o ajenas- en las que se represente o aparezca un menor.

  El delincuente trata de generar una confianza impostada, conseguida seguramente mediante la permanencia temporal, insistente, de constantes contactos a través de las TIC, para obtener el resultado (a través del embaucamiento) de establecer un encuentro o varios –una relación-, un cierto control emocional sobre el menor con escasa madurez sexual, para preparar -en el mundo virtual- el terreno para el abuso sexual –en el mundo real- o el delito de pornografía infantil (*sextorsión*) en que el proveedor sea el propio menor.

  Al castigarse en concurso delictivo el delito sexual, lo que este delito autónomo pena es el padecimiento psicológico, la intimidación de la cita, de la previa

insistencia, del chantaje para cometer otro delito de naturaleza sexual, obligado o mediante engaño.

En el **artículo 183 quater** del Código Penal se establece que, en los delitos de carácter sexual, si el autor es persona próxima en edad, grado de desarrollo o madurez a la víctima y se produce el delito con consentimiento libre de esta última, se excluye la responsabilidad penal, al entenderse que no concurre el abuso, ni pre valimiento que la diferencia de circunstancias suele propiciar.

3.2.4. Exhibicionismo y provocación sexual.

El exhibicionismo se encuentra tipificado en el **artículo 185** del Código Penal, estableciéndose pena para el que ejecutare o hiciere ejecutar a otra persona actos de exhibición obscena ante menores de edad o incapaces.

Respecto a la provocación sexual, el Código Penal castiga en el **artículo 186** al que, por cualquier medio directo, vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces.

3.2.5. Pornografía infantil.

Se encuentra regulada en el **artículo 189** del Código Penal, donde su bien jurídico protegido es el crecimiento armónico de la sexualidad del menor, el desarrollo normal de la madurez sexual del individuo como una cierta forma de proteger finalmente la defensa de la inocencia/pureza de la infancia (que aquí se coloca en una especie de pedestal defendible "*per se"*, explicando así que se penen como pornografía infantil, conductas que no inciden sobre menores concretos, como son las referentes a comics o montajes pornográficos, o la pornografía simulada, tras los cuales no hay ninguna persona real cuya sexualidad deba ser protegida).

La Decisión Marco 2004/68/JAI, del Consejo de 22/12/2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, pedía el endurecimiento de las penas para proteger al menor en base a su mayor vulnerabilidad y exposición a los

delitos, a la mayor dificultad que tiene para transmitir a los adultos su sufrimiento y sus problemas y en el mayor daño que estos delitos provocan tanto en su formación, como en su evolución sexual.

Está penado todo en relación con la pornografía del menor, desde su elaboración, hasta su difusión, favorecimiento o posesión, e incluso su visionado de propósito, aunque se penan según su intensidad y afección al menor, porque es la sexualidad armónica del menor lo que se protege, mediante muy heterogéneas conductas delictivas –unas con el menor y otras únicamente con su imagen- que van desde: captar, hasta usar menores/personas con discapacidad para participar en exhibiciones, crear pornografía, financiarla, producir, vender, distribuir, exhibir, ofrecer o facilitar la producción, venta, difusión o exhibición de la misma o poseerla con esos fines.

Se asimila a la pornografía de menores de 18 años, la de personas con discapacidad necesitadas de especial protección, obviamente, aunque superen la barrera de esa edad.

Inspirada en la Directiva 201/93/UE, se entiende por pornografía infantil la participación del menor o persona con discapacidad en una conducta sexual explícita –real o simulada-, o la representación de sus órganos sexuales con fin principalmente sexual –excluyendo el arte o el mero erotismo tolerado por las convenciones sociales, por ejemplo-, o la representación que parezca lo anterior, real o simulado, salvo que el representado al momento de su realización sea mayor de 18 años, y las imágenes realistas de la participación del menor o persona con discapacidad en una conducta sexualmente explícita o de sus órganos sexuales con fin principalmente sexual.

No importa que el origen del material sea en el extranjero, o fuere desconocido.

La pornografía infantil exige, en consecuencia, la existencia de un menor de edad -18 años, los aniñados de más edad son mayores-, real y la existencia de actos, imágenes o posturas no neutrales sexualmente (alcanzando la exhibición lasciva de genitales, por ejemplo) de modo que haya una acción sexuada ajena al propio menor o a su auto ideación, y descartando el simple desnudo –STS 8/03/2006, pero no el material que exhiba

lascivamente genitales o comportamientos sexuales-, la pornografía escrita y la oral, porque ésta siempre debe ser visual.

Ofrece dudas de punibilidad, por su desconexión con un concreto menor o persona con discapacidad y por lo tanto por la falta de bien jurídico concreto que proteger, la tipificación de las llamadas pornografía virtual y técnica; esto es, de imágenes realistas gráficas –comics, mantra, dibujos animados-, creaciones pornográficas artificiales, aunque sean muy parecidas a la realidad –hechas por ordenador-, y las simulaciones, pese a que lo diga el tipo penal, en que no habiendo exposición real de un menor, se construyen técnicamente –montajes-, pues alegar que de lo contrario se banalizaría o contribuiría a la explotación sexual, se acerca a penar conductas más anormales que penales -¿acaso alguien propondría penar las películas que simulan asesinatos u otros delitos?

No lo ofrecen, sin embargo, elementos como el número de contenidos que se transmiten, la estructura que se encuentre en el terminal, el número de veces en que se comporta la pornografía, la recepción de otros usuarios de la misma, la postura activa o meramente pasiva del enjuiciado, etc.

Son agravaciones específicas del delito básico, cuando concurra alguna de las siguientes circunstancias (art. 189.2 CP):

- Cuando se utilice a menores de dieciséis años.
- Cuando los hechos revistan un carácter particularmente degradante o vejatorio.
- Cuando el material pornográfico represente a menores o a personas con discapacidad necesitadas de especial protección que sean víctimas de violencia física o sexual.
- Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima.
- Cuando el material pornográfico fuera de notoria importancia.
- Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

- Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, del menor o persona con discapacidad necesitada de especial protección, o se trate de cualquier otro miembro de su familia que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad.
- Cuando concurra la agravante de reincidencia.

Además, en virtud del artículo 189.5 CP se pena con sanción menor:

- Adquirir o poseer pornografía infantil para uso propio.
- Acceder a sabiendas a pornografía infantil por medio de las TIC –lo que supone la punición del mero visionado de pornografía, salvo si es en soporte papel o es fortuito, sin intención o imprudente, por ejemplo-.

En el apartado 8 del citado artículo, se autoriza a los jueces (aún en fase de investigación, de manera cautelar y sólo a petición del Ministerio Fiscal, lo que excluye incluso a la Acusación particular) a la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español. Opción que igualmente se puede procurar –por otros legitimados, como la Acusación particular- por las vías del artículo 13 LECrim y del artículo 11 de la Ley 34/2012, de 11 de julio, de Servicio de la información y el correo electrónico.

Es delito comisible por persona jurídica, conforme dispone el artículo 189 bis CP.

3.2.6. Descubrimiento y revelación de secretos.

El «*hacking*» se le denomina al delito por el cual hay un acceso ilegítimo, de manera remota, al ordenador de un usuario (mediante virus troyanos, *botnets, spyware, keyloggers*, etc.). Este tipo de delito informático se denuncia ante nuestros Juzgados y Tribunales en un porcentaje del 4 %, incluyéndose la modalidad de *sexting* y/o sextorsión.

Es el delito tecnológico por excelencia –en el que no están penadas modalidades culposas- a través del cual se producen los mayores ataques a nuestra intimidad y privacidad almacenada actualmente en dispositivos tecnológicos –portátiles, tabletas o móviles- que sustituyen archivos, cajones, cartas y otras privacidades en formatos convencionales más de otros tiempos y a los que los hackers acceden sin permiso no ya solo como al comienzo de la era tecnológica por reto o diversión, sino también como los más modernos "*hackers by dollar*", que buscan y se apoderan de información, claves y datos ajenos para algo tan poco romántico como quedarse con nuestro dinero.

Se protege frente a ataques a la privacidad, o incluso poner en peligro la misma, adelantando la barrera penal de protección, mediante la interdicción de intrusiones o inmisiones principalmente de carácter técnico, que la colocan en situaciones de riesgo evidente, pues la privacidad supone poder excluir a terceros de la órbita de lo que uno preserva como íntimo.

Conductas tipificadas en el **artículo 197** CP, respecto a la intimidad personal:

- Apoderamiento inconsentido de correspondencia, documentos o mensajes de correo electrónico, o interceptación de telecomunicaciones o uso de artificios técnicos de escucha, transmisión, grabación o reproducción de audio o vídeo, para descubrir secretos de alguien o vulnerar su intimidad.
- Apoderamiento, uso o modificación no consentidos, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos; o acceder, alterar o utilizar los mismos –conformando los delitos básicos de descubrimiento-.
- Revelarlos, cederlos o difundirlos, aunque no se haya tomado parte en su indebida obtención, si se sabe de su origen ilícito.
- Se agravan las penas para las intrusiones que afecten a datos ultra protegidos –los que revelan ideología, religión, creencias, salud, raza o vida sexual-, personas especialmente protegidas –menores de edad o personas con discapacidad necesitada de especial protección- o cuando los realizan

encargados/responsables de los soportes informáticos o se ejecuten usando de forma no autorizada datos personales de la víctima o con fines lucrativos.

- Difundir, revelar o ceder a terceros imágenes o grabaciones audiovisuales sin autorización de la persona afectada, aunque se hayan obtenido con su anuencia inicial, obtenidas en un domicilio o lugar fuera del alcance de la mirada de terceros –sólo para la contemplación de determinada persona, no de cualquier persona, en el ámbito personal-, siempre que la divulgación menoscabe además gravemente su intimidad (piénsese, por ejemplo, en filmaciones eróticas o actos de carácter sexual) –conformando los delitos básicos de revelación-.

  Se protege en cierta forma la intimidad de quien la protege deficientemente, porque confía en cesionarios indiscretos o inmaduros, pues el material personal se cede a quien al final no es capaz de mantenerlo sin revelarlo.

  Es indiferente el móvil por el que se revela –muchas veces será la venganza tras la ruptura de relaciones afectivas-.

  El inicial consentimiento se trueca en mendaz –por el cambio radical de circunstancias contrario al principio "*rebús sic stantibus*", cuando cambia radicalmente el estado de una relación afectiva, por ruptura- de modo que es delictiva la divulgación de escenas de sexo explícito en que el divulgador es uno de los filmados, en lo que se refiere a los que no son él.

  Comparte algunas de las agravaciones anteriores, a las que aquí se suma que el autor sea el cónyuge o persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, por ser un ámbito, por la confianza que genera, de alto riesgo, como decimos, para estas inmisiones.

Conductas tipificadas en el **artículo 197 bis** CP, respecto a la privacidad como allanamiento informático:

- Acceder o facilitar a otro el acceso al conjunto o una parte de un sistema de información, sin autorización –desconocida, ignorada, subrepticia-, por

cualquier medio o procedimiento y vulnerando las medidas de seguridad impuestas, o

- Mantenerse en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, o
- Usar artificios o instrumentos técnicos, sin estar debidamente autorizado, para interceptar transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos –emisiones o transmisiones entre sistemas, diálogos entre maquinas no humanas, transmisiones automáticas entre equipos, maquinas cuyos rastros y datos pueden dar información sobre costumbres privadas de un usuario (por ejemplo, si hay conexión con un router o si se está con un aparato encendido, que pueden dar información locativa o temporal sobre las costumbres de una persona).

Característica común a los tipos aquí incluidos y los del precepto anterior es la ausencia del consentimiento de la víctima que tolera las intrusiones –a veces mediante fórmulas tácitas- en consonancia con el renunciable derecho a la privacidad, imagen, secreto de las telecomunicaciones y protección de datos reservados del artículo 18 CE, pues si el afectado lo presta, o la protección del dato o sistema informático es socialmente tenida por deficitaria –teoría de la expectativa razonable de privacidad-, no hay delito.

Sin embargo, en este segundo precepto, el ataque a la privacidad se produce por un modo de "allanamiento informático" –que puede ser *hacking blanco*-, esto es, se pena la mera intrusión en esferas tecnológicas en donde normalmente se guardan privacidades e intimidades –eso sí, con dolo reduplicado, pues a la no autorización expresa para acceder o mantenerse, se suma la vulneración de las claves de protección impuestas al sistema, y aunque sean favorecedoras, facilitadoras de posibles ulteriores ataques a la intromisión-, de modo que no es imprescindible que estas se hallen llenas de contenidos, ni que estos sean secretos "*strictu sensu*", porque la protección legal de la privacidad es aquí meramente formal –no material-, y se hace al medio, por la antijuridicidad que revelan los medios y no tan sólo al contenido, lo mismo que el allanamiento de morada protege una realidad distinta de la propiedad que pueda haber dentro de una casa.

Conductas tipificadas en el **artículo 197 ter** CP:

- Producir, adquirir para usar –y no meramente poseer o detentar, como en el artículo 248.2 b) CP-, importar o, de cualquier modo, facilitar a terceros, sin estar debidamente autorizado:
  - Un programa informático, concebido o adaptado principalmente para cometer cualquier delito de los anteriores; o
  - Una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Todas estas modalidades de protección contra ataques tecnológicos contra las diversas manifestaciones de nuestra privacidad, se conciben como delitos semipúblicos, y en consecuencia, exigen denuncia previa del ofendido –salvo que afecten a intereses generales ¿compatibles con lo privado? o a una pluralidad de personas- y su perdón sólo extingue la acción penal, no la pena.

De conformidad con lo recogido en el artículo 197 quinquies CP, son delitos comisibles por persona jurídica.

3.2.7. Calumnias e injurias.

Delitos tradicionales vehiculizados a través de Internet, aunque en la actualidad suponían un 4,6% de los que llegaban a nuestros Juzgados y Tribunales, cada vez se denuncian más, sobre todo una vez despenalizadas las faltas equivalentes, y eso que como delitos privados que son, solo son perseguibles a instancia de parte legitimada, por lo que exigen las formalidades de los artículos 215 CP y 804 LECrim: querella y acto de conciliación, y si son vertidas en juicio, licencia judicial.

Desaparecida como falta, la que antes lo era –la leve-, en la actualidad, debe continuar siendo impune, quedando como delictiva, la que por su naturaleza, efectos y

circunstancias, siga siendo tenida en el concepto público por grave –**artículo 208.2** CP- o hecha con temerario desprecio a la verdad –**artículo 208.3** CP-.

Las ofensas, vilipendios, vejaciones, escarnecimientos, menosprecios peyorativos, etc. que se producen a través de nuevas tecnologías, especialmente las que se publican en blogs, webs, redes sociales abiertas, inicialmente son delictivas, pues normalmente alcanzan gran difusión, reforzando el ataque contra la estimación social, fama, consideración, honor y dignidad inherente al ofendido, que requiere el delito.

La red permite divulgar cualquier mensaje en pocos segundos, lo hace a una multitud de usuarios de carácter muy diverso que está situados incluso en países lejanos, obteniendo una publicidad de los mensajes –y con ello un ataque reduplicado a la consideración social del afectado- impensable hace tan solo unos pocos años.

Sin embargo, los exabruptos, chistes dañinos, comentarios vejatorios y menospreciantes, etc. cuando se vierten a distancia entre personas que no se conocen entre sí, y si no se reiteran, pueden ser tenidos como meros desahogos impunes, a modo de simples "comentarios de café" que, pese a su difusión en entornos accesibles a mucha gente, no son tenidos como injuriosos, en la aplicación del principio de intervención mínima.

Si la acción se da en un contexto de violencia de género, aun cuando la injuria o vejación injusta sea leve –ex artículo 173.4 CP- es delictivo.

La reparación del daño generado por infracciones de esta entidad realizadas en medios de gran difusión pública –como son los digitales-, comprende también la publicación o divulgación de la sentencia condenatoria –artículo 216 CP-, a costa del condenado en medios, horarios y circunstancias equivalentes a las que concurrían a la hora de vejar la dignidad ajena.

Si la finalidad menospreciante concurre con móviles que inciten a la violencia contra el injuriado, en razón de diferencias propias de la intolerancia, es de preferente aplicación del artículo 510 CP.

Tanto en estos dos tipos de delitos, como en los de enaltecimiento, los comportamientos activos posteriores neutralizantes, –prolongados en el tiempo, con publicidad y emitidos en medios o foros semejantes- que exterioricen arrepentimientos visibles, deben poder valorarse para reducir o incluso evitar la condena.

3.2.8. Daños informáticos.

El Código Penal establece en su **artículo 264.1** que será castigado el que por cualquier medio, sin autorización y de manera grave, borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave. Asimismo, el **artículo 264 bis** CP en su apartado 1 castiga al que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo 264.1
b) introduciendo o transmitiendo datos; o
c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si bien este mismo artículo, en su apartado 3, prevé una agravación de la pena prevista cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

3.2.9. Usurpación de identidad.

La suplantación de la personalidad ajena, en la que uno se hace pasar por otro –muy propia de la cobardía de ciertos delincuentes informáticos- no es delito autónomo en España, como lo es en otros sistemas jurídicos en Derecho comparado, al no conformar en sí misma, la suficiente entidad penal.

No se puede confundir con el delito de usurpación del estado civil del artículo 401 CP, pues esta exige una clara suplantación constante de alguien por otro mediante acciones no solo virtuales y esporádicas, -casi siempre puntuales en las estafas- con intención total de permanencia temporal.

Sin embargo, el hacerse pasar por otro suele formar parte de la descripción de ciertos elementos de otros tipos penales, en operaciones concretas, formando parte del delito: como es el caso del engaño bastante en los "*phishing*", o en algunos ofrecimientos sexuales de tercero, o en algunas maneras de conseguir el contacto preciso para el delito de "*chilgrooming*" o el acoso del "*stalking*", etc.

3.2.10. Incitación al odio y violencia contra grupos.

El odio es un sentimiento interno que queda en sí fuera del reproche penal –el pensamiento no delinque-, no así su exteriorización, con mensajes inequívocos de apoyo a la violencia contra otros colectivos/individuos diferentes, que sobrepasa el límite a la libertad de opinión, la ironía, la polémica o la mera critica, incidiendo en actuaciones que causan grave daño a los colectivos afectados.

Es delito, en consecuencia:

- Fomentar, promover o incitar.
- Directa o indirecta, pero públicamente.
- Al odio, hostilidad, discriminación o violencia.
- Contra un grupo, parte de él o un individuo determinado.
- Por razón de su pertenencia a él por racismo, antisemitismo, ideología, religión o creencias, situación familiar, pertenencia a una etnia, raza o nación, su origen nacional, su sexo, orientación/identidad sexual, género, enfermedad o discapacidad.

También lo es:

- Elaborar, poseer para distribuir, mover escritos u otro material idóneo para fomentar/promoverlo.

- Públicamente negar, trivializar gravemente o enaltecer el genocidio, la lesa humanidad, los delitos en conflicto armado, ya cometidos, si promueven o favorecen un clima de violencia, hostilidad, odio o discriminación.
- Lesionar la dignidad de personas mediante acciones de humillación, menosprecio, descrédito de los grupos o individuos anteriores o posean material idóneo para hacerlo.
- Enaltecer o justificar por medio público o de difusión los delitos anteriores cometidos, o a sus autores.

Configura como agravantes:

- Cometerlo a través de un medio de comunicación social, por medio de Internet o mediante el uso de tecnologías de la información, de modo que, aquel se hiciera accesible a un elevado número de personas.
- Cuando los hechos, a la vista de sus circunstancias, resulten idóneos para alterar la paz pública o crear un grave sentimiento de inseguridad o temor entre los integrantes del grupo.

La pena se acompañará, en todos los casos, de la pena de inhabilitación especial para profesionales relacionados con la docencia, ocio, educación o deporte.

El juez o tribunal acordará la destrucción, borrado o inutilización del material y soporte objeto del delito o por medio de los cuales se hubiera cometido. Cuando el delito se hubiera cometido a través de TIC, se acordará la retirada de los contenidos.

En los casos en los que, a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos a que se refiere el apartado anterior, se ordenará el bloqueo del acceso o la interrupción de la prestación del mismo.

Aunque el delito no permite específicamente esas medidas informáticas judiciales restrictivas expresamente en la fase de instrucción, al modo como lo hacen ex profeso los artículos 189.8, 578.5 y 579.4 CP, se puede entender por su contexto que ésta no es una facultad exclusiva del juez del fallo, como ocurre en el artículo 270.3 CP.

De conformidad con lo prevenido en el artículo 510 bis CP, este es delito comisible por persona jurídica.

4. CUESTIONES PRÁCTICAS Y PROCESALES RELACIONADAS CON LA INVESTIGACIÓN DE LOS DELITOS INFORMÁTICOS[17].

4.1. Competencia territorial y persecución internacional.

4.1.1. Principio de ubicuidad.

A la hora de perseguir determinados delitos cometidos por medios informáticos se plantean ciertas dudas sobre el lugar de comisión de los mismos, habida cuenta que la acción o la comunicación delictiva se realiza desde un emplazamiento o lugar en muchas ocasiones ignorado, a través de un ordenador u otro equipo con acceso a internet, que no siempre está fijo, y que puede redireccionar a través de diversos servidores ubicados en lugares y países diversos, pudiendo producirse los efectos en muchos y muy diversos emplazamientos físicos, muchas de las veces llegando a ocupar un ámbito internacional.

Para evitar discusiones estériles en materia de competencia, nuestro Tribunal Supremo (en adelante TS) viene considerando que el delito informático, que normalmente se comete desde un ignorado lugar y produce sus efectos en diversas ubicaciones geográficas, se produce y por tanto es competente para su persecución en todos y cada uno de los sitios donde se manifiestan sus efectos, lo que incluye tanto el lugar de la acción como el del resultado.

Esta opción sobre competencia territorial se conoce como principio de ubicuidad, y se adoptó de forma casi unánime y reiterada a partir del **acuerdo no jurisdiccional** del

[17] Disponible en: http://181.189.159.2/2014/septiembre/prueba/contenido/ponencias/Anexos/Legislacion/Cuestiones%20practicas%20y%20procesales%20investigacion%20delitos%20informaticos.pdf [consulta: 10/04/2018].

pleno del **TS de 03/02/2005**, según el cual: *"el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa"*. Esta regla se establece de forma inicial. Si avanzada la investigación de la causa llegara a determinarse el lugar geográfico concreto desde el que se introdujeron los datos delictivos en la red, cabe la inhibición a favor del Juez así determinado, ello conforme a la regla general del *fórum delicti comisi* del artículo 14 de la LECrim.

Por otro lado, respecto del delito de injurias cometido en un foro de internet y en el que planteó cuestión negativa de competencia entre los Juzgados del domicilio del denunciante y aquél en que radicaba el servidor de la página web, el Auto del TS de 12/01/2012 (Rº 20591/11), atribuyó la competencia, en base al principio de ubicuidad, al Juzgado en el que se habían iniciado las actuaciones, lugar del domicilio del denunciante y ofendido y lugar donde se reciben las ofensas. Dicha resolución vino a establecer expresamente que: *"… el criterio de que en los delitos cometidos a través de internet serán competentes los juzgados en los que se haya introducido en la red los contenidos delictivos, se refiere a los delitos de pornografía infantil, pero siempre ha sido matizada cuando nos encontramos con delitos de diferente naturaleza como en el caso que nos ocupa de las injurias, ya sea vía internet o telefónica, al igual que en el caso de los daños informáticos, delito de resultado que no se comete desde donde se lanza el ataque sino donde se produce los daños, se destruye el sistema operativo o se contaminan los archivos …"*.

4.1.2. Principio de universalidad.

Por regla general, los delitos informáticos no tienen la consideración de delitos de persecución internacional, pues no se encuentran comprendidos entre los que el artículo 23.4 de la LOPJ[18] incluye entre esa categoría.

No obstante, el carácter internacional de algunos de los delitos informáticos, se aprecia claramente en el de **pornografía infantil** (artículo 190 del CP), el cual es de persecución universal en base a una doble vía:

[18] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

a) Por ser delitos contra la libertad e indemnidad sexual cometidos sobre víctimas menores de edad, en virtud del art. 23.4.k) de la LOPJ.
b) Por establecer el artículo 189.1.b) del CP para los delitos de tráfico de material pornográfico infantil que es indiferente que el mismo tenga su origen en el extranjero o fuere desconocido.

Pese a ser delitos de persecución universal, que podría hacer pensar que la competencia para su instrucción correspondería a los Juzgados Centrales de Instrucción, sin embargo, la misma se atribuye a los Juzgados de Instrucción en base al ya examinado principio de ubicuidad.

4.2. Interrupción de la prescripción.

La peculiaridad fundamental que afecta a estos delitos es que tienen una penalidad no muy elevada, lo que obliga a una cierta celeridad en su investigación pues, de lo contrario, podrían prescribir; además, las huellas y pistas que su comisión dejan desaparecen y se difuminan rápidamente, pues no podemos olvidar que los datos de tráfico de las comunicaciones que sirven de vestigio desaparecen rápidamente, toda vez que la obligatoriedad de la conservación de tales datos no es la misma en todos los países[19]; además, las posibilidades de averiguar la autoría de la infracción disminuyen rápidamente conforme pasa el tiempo.

Tras la reforma operada en el artículo 131 del CP por la LO 5/2010, de 22 de junio, se ha ampliado el plazo mínimo de prescripción que ha pasado de los tres a los cinco años. La prescripción se interrumpe cuando el procedimiento se dirija contra la persona indiciariamente responsable del delito.

Dicha persona indiciariamente responsable deberá quedar suficientemente determinada en la resolución judicial, ya sea mediante su identificación directa o mediante datos que permitan concretar posteriormente dicha identificación en el seno de la

[19] 12 meses como máximo para España, según lo establecido en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

organización o grupo de personas a quienes se atribuya el hecho. Es decir, siguiendo la doctrina emanada de nuestro Tribunal Supremo, el legislador ha optado no sólo por la identificación directa (nombre y apellidos del denunciado), sino también por la identificación indirecta siempre y cuando se permita su posterior filiación completa a lo largo del procedimiento.

En los delitos informáticos bastaría con conocer la dirección IP a cuyo través se cometió el delito, para tener por interrumpida la prescripción; pues, en principio, a través de la misma se podría llegar a determinar la persona indiciariamente responsable.

4.3. Obtención de datos de tráfico.

4.3.1. Contenidos protegidos por el secreto de las comunicaciones.

Desde la perspectiva subjetiva, los titulares del secreto de las comunicaciones pueden ser tanto las personas físicas como las jurídicas, nacionales o extranjeras, "porque el secreto de las comunicaciones presupone la libertad, y su restricción se produce en un sentido de control y observación y no propiamente de impedimento a las comunicaciones" (vid. STS nº 246/1995, de 20 de febrero, STC nº 114/1984, de 29 de noviembre).

También **los menores** son titulares del derecho al secreto de las comunicaciones. La LOPJM[20], les reconoce en su artículo 4 este derecho y encomienda a los padres o tutores y a los poderes públicos respetarlo y protegerlo frente a ataques de terceros, todo ello sin perjuicio de las modulaciones derivadas del ejercicio legítimo de la patria potestad o de la tutela.

El **Convenio** número 185, del Consejo de Europa, **sobre Ciberdelincuencia**, de 23 de noviembre de 2001, ratificado por el Estado español, también define los datos de tráfico de forma amplia en su artículo 1.d) como todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en

[20] LO 1/1996, de 15 de enero, de Protección Jurídica del Menor.

cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, el tiempo, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. Esta definición se apoya en una dependencia temporal y funcional de los datos de tráfico con respecto a la comunicación.

La identificación del terminal o terminales objeto de injerencia ha pasado a ser un componente esencial de cualquier título habilitante; su omisión, como nos advierte la STS nº 201/2006, de 5 de marzo, podría dar lugar a la apreciación de un vicio en el título de raigambre constitucional, con potencialidad de extender su fuerza anulatoria a todas las pruebas directas y derivadas relacionadas con la información obtenida del contenido de las comunicaciones interceptadas.

La previa identificación del titular de un número, que luego resulta intervenido, no es indispensable para la legitimidad de la injerencia (SSTS nº 493/2011, de 26 de mayo y 309/2010, de 31 de marzo).

Como declara la STC nº 150/2006, de 22 de mayo: *"a la vista de los avances tecnológicos en el ámbito de la telefonía –por ejemplo, con la aparición de teléfonos móviles y tarjetas prepago, que dificultan la identificación de los titulares y usuarios, facilitando el intercambio de los teléfonos- esas exigencias resultarían desproporcionadas por innecesarias para la plena garantía del derecho y gravemente perturbadoras para la investigación de delitos graves, especialmente cuando éstos se cometen en el seno de estructuras delictivas organizadas".*

Por tanto, la persona investigada no tiene que ser necesariamente titular del terminal objeto de injerencia (SSTC nº 1154/2005, de 17 de octubre, 934/2004, de 15 de julio; 463/2005, de 13 de abril y 918/2005, de 12 de julio).

Debe en este punto recordarse la obligación a los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago de llevar un libro-registro[21] en el que conste la identidad

[21] Disposición Adicional Única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones

de los clientes que las adquieran y que los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

El TS ha llegado a admitir la intervención del teléfono de un tercero no implicado cuando se sospecha fundadamente, que puede ser utilizado para enviar o captar mensajes o mantener conversaciones cuyo contenido puede tener intereses para la investigación en marcha si bien en este caso deberá extremarse la motivación, ya que se afecta, al mismo tiempo, al derecho a la intimidad y secreto de las comunicaciones de personas que, en principio, no están directamente implicadas en las investigaciones en marcha (STS nº 960/1999, de 15 de junio).

4.3.2. Revelación de datos por uno de los interlocutores.

Las grabaciones de las conversaciones por uno de los interlocutores no afectan al secreto de las comunicaciones, sino al **derecho a la intimidad**, por lo que pueden articularse como prueba aunque se hayan efectuado sin autorización judicial (vid. SSTS nº 208/2006, de 20 de febrero, 1564/1998, de 15 de diciembre, 1354/2005, de 16 de noviembre; STC nº 56/2003, de 24 de marzo).

La garantía del secreto de las comunicaciones sólo opera cuando la injerencia es realizada por una persona ajena al proceso de comunicación, ya que lo que persigue la norma es garantizar la impenetrabilidad de la comunicación por terceros ajenos a la misma. Como declara la STC nº 56/2003, de 24 de marzo: *"la presencia de un elemento ajeno a aquéllos*

entre los que media el proceso de comunicación, es indispensable para configurar el ilícito constitucional aquí perfilado".

4.3.3. Utilización del teléfono intervenido por terceras personas.

Debe abordarse el problema del tercero o "comunicante accidental"; esto es, la persona que no es directamente investigada pero que entabla comunicación telefónica con el investigado.

En efecto, una intervención telefónica puede afectar los derechos de terceros ajenos a la investigación, sin que ello genere nulidades. La STS nº 433/2012, de 1 de junio, puntualiza que la intervención afecta a las comunicaciones de las personas investigadas, pero puede suponer la inclusión como prueba de cargo las manifestaciones de los que se comuniquen con ellos, siempre que se refieran al hecho delictivo objeto de investigación.

4.3.4. Acceso a los datos internos de los teléfonos móviles.

A tales efectos debe distinguirse entre acceso a la libreta de direcciones (agenda telefónica) y acceso al registro de llamadas. En este sentido, cuando el acceso de la Policía al teléfono móvil del investigado se limita a los datos recogidos en el archivo de contactos telefónicos, pero no en el registro de llamadas efectuadas y/o recibidas, debe concluirse que dichos datos no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros. Con el acceso a la agenda de contactos telefónicos no se obtiene dato alguno concerniente a la transmisión de comunicación emitida o recibida por el teléfono móvil, sino únicamente un listado de números telefónicos introducidos voluntariamente por el usuario del terminal sobre los que no consta si han llegado a ser marcados.

Desde luego, los mensajes enviados al destinatario pero aún no leídos por éste deben entenderse protegidos por el derecho al secreto de las comunicaciones.

Existen dudas en torno a si el acceso a los mensajes acumulados en la memoria del teléfono móvil de un detenido supone o no una injerencia en el derecho al secreto de las

comunicaciones o, si por el contrario, en estos casos el único derecho afectado es el derecho a la intimidad de la persona investigada, interpretación esta última que permitiría actuaciones de injerencia proporcionadas a las circunstancias del hecho y de la investigación.

4.3.5. Datos relativos al IMEI.

El término IMEI (*International Mobile Equipement Identity)*, como el similar IMSI (*International Mobile Subscriber Identity)*, designan un código de identificación único para cada dispositivo de telefonía móvil, representado por una serie de algoritmos, que se integra en la tarjeta SIM y que permite su identificación a través de las redes GSM y UMTS, el cual está formado por el código del país concernido –que se compone de tres dígitos-, el código de la red móvil –compuesto de dos dígitos-, y un número de diez dígitos que contiene la identificación de la estación móvil, pero que no contiene el número concreto del teléfono del abonado.

Tanto el IMEI como el IMSI carecen de capacidad de información sobre la identidad del usuario, teniendo valor probatorio únicamente si se asocia a otros datos en poder de las operadoras.

La captación de tales números a efectos de investigación penal es posible mediante un escaneado o barrido realizado a través de instrumentos electrónicos que detectan aquellos siempre que se actúe en un determinado radio de acción en el que se encuentra el terminal telefónico. Su captación se realiza, por tanto, como consecuencia de un seguimiento dirigido específicamente frente a un individuo o individuos determinados.

Con posterioridad a la captación, una vez obtenido el correspondiente código identificativo, es necesaria la obtención del número comercial del teléfono, en posesión de la prestadora del servicio de telecomunicación. Tanto con el IMSI como con el IMEI se dispone de información suficiente como para poder solicitar la autorización judicial de identificación por el operador de los números de teléfono (o MSISDN) que corresponden a tales datos, y la correspondiente intervención de las conversaciones. Ni el IMSI ni el IMEI por sí solos, son datos integrables en el concepto de comunicación.

Sin embargo, no puede la Policía solicitar tal información de las operadoras. Es precisa, pues, autorización judicial para la cesión del IMSI y del IMEI por las operadoras, no porque se integren dentro del marco protector del secreto de las comunicaciones sino porque la Ley 25/2007, de 18 de octubre, así lo exige.

4.3.6. Investigación de la dirección IP.

Una dirección IP es una etiqueta numérica que identifica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP (*Internet Protocol)*, que corresponde al nivel de red del protocolo TCP/IP. El IP no identifica por sí al usuario.

El principio básico es el de que no se precisa autorización judicial para conseguir lo que es público. El TS considera que estos datos no se encuentran protegidos ni por el artículo 18.1 CE, ni por el art. 18.3 CE (SSTS nº 292/2008, de 28 de mayo; y 776/2008, de 18 de noviembre). Tras la averiguación del IP, las subsiguientes actuaciones de identificación y localización de quién sea la persona que tiene asignado ese IP se deben llevar a cabo bajo control judicial.

Debe, no obstante, tenerse presente una matización: la jurisprudencia distingue, por un lado, los casos de rastreo policial del espacio público y, por otro lado, los supuestos en los que para acceder a una información sobre IP es necesario oficiar a una operadora. En este último supuesto, sí debe considerarse necesario obtener autorización judicial conforme a las previsiones de la Ley 25/2007, de 18 de octubre (SSTS nº 292/2008, de 28 de mayo; 236/2008, de 9 de mayo; 680/2010, de 14 de julio).

4.3.7. Acceso al correo electrónico.

Puede decirse que existe una *communis opinio* en orden a considerar al *e-mail* como un medio asimilable al teléfono, a efectos de aplicarle idénticas garantías procesales penales.

A estos efectos debe aplicarse el mismo régimen a las diversas modalidades de mensajería instantánea (*instant messaging)* cuyo uso generalizado ha colocado a este medio en pieza esencial en las comunicaciones interpersonales (*v.gr. whatsapp o skip).*

El acceso a un correo electrónico que aún no ha sido leído por su receptor, con independencia del momento concreto del proceso de comunicación en que se encuentre (ya esté escrito y almacenado en el ordenador personal, o en el terminal telefónico pendiente de ser enviado a su destinatario final, o enviado y recibido pero aún no leído), pero siempre durante dicho proceso, supone sin duda una injerencia en el secreto de las comunicaciones.

En todo caso, dado lo difícil de deslindar uno y otro tipo de correo, razones de prudencia deben llevar a solicitar la autorización judicial para acceder a cualquier mensaje enviado por correo electrónico. Esta conclusión se refuerza por el hecho de que el TC ha otorgado protección a los datos externos del proceso comunicativo aunque el mismo hubiera ya concluido. Si se protegen los datos externos del proceso comunicativo concluso, con más razón habrá de otorgarse protección al contenido de la comunicación finalizada.

La intervención de correo electrónico exige que la resolución judicial especifique las concretas cuentas de correo electrónico afectadas, no siendo una buena práctica la de reseñar la línea telefónica habitualmente utilizada por el sujeto pasivo de la medida, ya que el mismo puede acceder a su cuenta o cuentas de correo electrónico a través de otras líneas.

4.3.8. Cesión de datos almacenados por las operadoras.

La cesión de tales datos por las operadoras se subordina conforme al artículo 1.1 de la Ley 25/2007, de 18 de octubre, a "*la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales*". En definitiva, con el marco jurídico vigente, toda investigación policial o del Ministerio Fiscal para el esclarecimiento de un hecho delictivo que requiera la cesión de alguno de los datos almacenados por las operadoras impondrá de forma incuestionable autorización del Juez de Instrucción.

Debe en este punto recordarse que, conforme al Acuerdo del Pleno no jurisdiccional de la Sala 2ª del Tribunal Supremo de 23/02/2010, "*es necesaria la autorización judicial para que las operadoras que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el artículo 3 de la Ley 25/2007, de 18 de octubre*".

Por otra parte, la Ley 25/2007 introduce confusión al restringir la posibilidad de cesión a la averiguación de delitos graves. Una interpretación literal, conforme al concepto de delito grave contenido en el artículo 33 CP, podría dejar impunes múltiples delitos cometidos por Internet o telefonía. Una interpretación teleológica ha de llevar al entendimiento de que la gravedad debe definirse en atención a las circunstancias concretas del hecho, teniendo en cuenta el bien jurídico protegido y la relevancia social de la actividad, de conformidad con la jurisprudencia recaída en relación con los delitos susceptibles de ser investigados mediante intervenciones telefónicas/telemáticas.

Una interpretación sistemática conduce a la misma conclusión: ningún sentido tendría imponer mayores restricciones a la cesión de datos externos que al acceso al contenido de lo comunicado.

Limitar el ámbito de la Ley 25/2007 a los delitos graves, tal y como se definen en los artículos 13 y 33 CP, supondría en realidad frustrar tanto la finalidad perseguida por la Directiva 2006/24/CE como el objetivo de la Convención sobre Ciberdelincuencia del Consejo de Europa, que es precisamente posibilitar la investigación de los delitos que se sirven de las tecnologías de la información y la comunicación.

Es constatable que la opción de nuestro legislador ha dado pie a interpretaciones que siguiendo el tenor literal del precepto, restringen el acceso a los delitos graves, tal y como se definen en los artículos 13 y 33 CP. Ni que decir tiene que seguir esta interpretación supone cortar de raíz la posibilidad de investigar conductas que utilizando tecnologías de la información y la comunicación y teniendo gran trascendencia social, no alcanzan, por la penalidad asignada, el rango de delito grave.

4.3.9. Conversaciones en chats.

Existen otros medios en Internet, como los chats o foros, que permiten comunicarse a varias personas simultánea y públicamente, en tiempo real.

En estos casos, cuando las conversaciones o comunicaciones son accesibles para cualquier usuario de Internet, las mismas no pueden tener la consideración de conversaciones privadas. Por ello, estas modalidades no pueden considerarse comprendidas dentro del ámbito del derecho fundamental al secreto de las comunicaciones, por lo que no precisan de autorización judicial para su grabación u observación.

Distinto habrá de ser el tratamiento de los supuestos en los que se use la opción de comunicación bidireccional cerrada entre dos usuarios, pues en estos casos, conforme a la propia naturaleza del acto comunicativo, deben activarse de nuevo las garantías del artículo 18.3 CE.

4.3.10. Acceso a contenidos y datos almacenados en discos duros.

La apertura de archivos de un disco duro o de unidades externas tampoco afecta al derecho al secreto de las comunicaciones. Se considera más bien el cuerpo de los delitos informáticos. Por ello, no es en todo caso imprescindible la autorización judicial, a salvo, como ya se expuso, el acceso a correos electrónicos.

Los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos bien en teléfonos móviles, ordenadores o asimilados, tendrían la consideración de simples documentos y, por tanto, sólo resultarían, en su caso, protegidos por el derecho a la intimidad (STS nº 782/2007, de 3 de octubre).

Por ello, las FCSE pueden, sin autorización judicial, intervenir un soporte magnético o electrónico, como, por ejemplo, la lectura de un disco duro, aún cuando su contenido material pudiera afectar al derecho a la intimidad del artículo 18.1 CE, si se

aprecian razones de urgencia y se persigue un interés constitucionalmente legítimo con base en la habilitación legal para dicha actuación reconocida en los artículos 282 LECrim y 11.1 LOFCS 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad; así como, en el artículo 547 LOPJ. En este sentido, vid. STC nº 173/2011, de 7 de noviembre, en relación con la investigación de un delito de pornografía infantil. Esta doctrina sería también aplicable a las unidades de almacenamiento externo, PDA y asimilados.

4.4. Convenios Internacionales en la materia.

4.4.1. El Convenio de Budapest sobre cybercrimen.

El Consejo de Europa puso en Budapest a disposición de los Estados el día 23/11/2001 para su ratificación, el Convenio del Cybercrimen (delitos informáticos) redactado por los países de la Unión Europea, más USA, Canadá, Japón y África del Sur, con el propósito principal de adoptar una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

Dicho Convenio está en vigor para España desde el día 01/10/2010, habiendo sido publicado en el BOE de 17/09/2010, y tiene un alto interés jurídico, por cuanto además de perseguir vocación universal, es el primer Tratado Internacional sobre delitos contra sistemas, datos o redes informáticos, y pretende armonizar el Derecho sustantivo, los instrumentos para facilitar su persecución y la cooperación internacional en esta materia, sistematizando los medios de investigación en esta materia, sobre los que nos vamos a centrar.

a) **Conservación rápida de datos informáticos almacenados:** se trataría de datos preexistentes, ello mediante orden judicial (mandamiento) a proveedor de servicios de acceso a Internet. Siendo necesario que haya en curso una investigación penal, de modo que se prohíben cualquier tipo de exploraciones de carácter prospectivo o intuitivo. Los datos conservables, son tanto de tráfico como de contenido (haciendo especial hincapié en los delitos relacionados con la pornografía infantil),

todo ello con el objeto de obtener pruebas. La conservación será por 90 días prorrogables por otro período igual, imponiéndose tanto a los custodios y ordenantes el deber y la obligación de secreto de lo que se está haciendo y de que hay una investigación en curso. Todo ello se consigue mediante la entrada secreta del local donde se encuentra el sistema informático y registrando el mismo, así como mediante la orden a la empresa servidora de conservación de los datos, con el oportuno secreto y sigilo.

b) **Conservación inmediata y revelación parcial de datos de tráfico:** ello para conocer a través de esos datos de tráfico intermedio el origen, destino y camino seguido por el infractor.

c) **Mandamientos de exhibir:** obligan a suministrar determinados datos informáticos preexistentes a los suscriptores a un proveedor informático.

d) **Registro y decomiso de datos informáticos:** equivalente a la entrada y registro, pero con la particularidad de la custodia de datos intangibles y la extensión a otros ordenadores de Red o sistema unidos al que registra. Además se puede embargar el hardware (programas necesarios para el acceso a datos decomisables y aseguramiento de datos mediante su extracción y volcado).

e) **Interceptación de datos de tráfico y contenido en tiempo real:** en los que se exige deber de secreto/sigilo en quien los ejecute, al ser más restrictivos de derechos fundamentales.

4.4.2. Cooperación jurídica internacional y policial.

Cuando se trata de analizar intervenciones obtenidas a través de cooperación internacional es fundamental conocer la norma procesal que rige la ejecución de la diligencia solicitada.

La regla tradicional en cooperación internacional es la ejecución de las diligencias solicitadas conforme a la norma procesal del país de ejecución (*lex loci).* Así, el artículo 3.1

del Convenio Europeo de Asistencia Judicial en materia penal del Consejo de Europa de 20 de abril de 1959 dispone que *la Parte requerida hará ejecutar, en la forma que su legislación establezca, las comisiones rogatorias relativas a un asunto penal que le cursen las autoridades judiciales de la Parte requirente y que tengan como fin realizar actuaciones de instrucción o transmitir piezas probatorias, expedientes o documentos.* Esta misma regla es la que contienen la mayoría de los Convenios bilaterales en materia de asistencia judicial en materia penal.

El nuevo art. 4 del Convenio de Asistencia Judicial Penal entre los países miembros de la , de 29 de mayo de 2000, introduce la posibilidad de solicitar el respeto a determinadas formalidades de la *lex fori*, al disponer que *en los casos en los que se conceda la asistencia judicial, el Estado miembro requerido observará los trámites y procedimientos indicados expresamente por el Estado miembro requirente, salvo disposición contraria del presente Convenio y siempre que dichos trámites y procedimientos no sean contrarios a los principios fundamentales del Derecho del Estado miembro requerido.* No obstante, se mantiene básicamente el respeto a la *lex loci* en la regulación específica de la intervención de comunicaciones contenida en los artículos 17 a 22.

En general de un examen detallado de la jurisprudencia del TS en relación con estas pruebas se deducen tres principios generales:

1. Que la prueba internacional obtenida conforme a la norma procesal del país donde se obtuvo no debe ser sometidas al tamiz de su conformidad con las normas españolas.
2. Quedaría abierta la posibilidad de valorar si esas pruebas fueron practicadas conforme a las normas procesales del país de obtención. En este caso, corresponde a quien lo alega la prueba de la inobservancia de la norma procesal extranjera y por tanto de la ilegalidad y nulidad de esta prueba.
3. En el ámbito europeo, el Tribunal Supremo español ha añadido un criterio general de confianza en las garantías comunes vigentes en el espacio judicial europeo.

Existe una modulación de esta doctrina general: tras declarar el TS que "la doctrina de esta Sala ha establecido que la legalidad de las actuaciones policiales o judiciales que se desarrollan en otros países no corresponde valorarlas a los Tribunales españoles conforme a las normas internas, pues son las leyes vigentes en cada lugar las que deben ser

observadas por sus autoridades locales en el cumplimiento de sus funciones", se establece que "esta afirmación de carácter general admite algunas matizaciones. De un lado, ha de considerarse referida, inicialmente, a países en los que se mantengan de modo efectivo los mismos valores y principios que en España se consagran en la Constitución, de manera que las exigencias para la restricción de los derechos de los ciudadanos sean material y sustancialmente similares. En segundo lugar, para que pueda avanzarse en el cuestionamiento de esas actuaciones sería preciso aportar un dato objetivo de una posible infracción de derechos fundamentales no tolerable por nuestro ordenamiento" (STS nº 1099/2005, de 30 de septiembre). Por otro lado, "la ausencia de garantías en relación con los actos practicados en el extranjero debe ser probado por quien lo alega" (STC nº 155/2001).

5. LA PRENCIÓN Y CONCIENCIACIÓN COMO PILAR FUNDAMENTAL.

La prevención en el ámbito del uso de la tecnología, se convierte en un elemento fundamental cuando estamos hablando de su uso por menores.

Pero para poder ayudar a los menores a prevenir, hay que tener en cuenta que el llamado *inmigrante digital* (los adultos que han llegado a Internet de la mano de la necesidad o del trabajo a la tecnología), también tiene que conocer tanto o más el uso y, sobre todo, el funcionamiento de la Red y, especialmente, de las redes sociales.

Esta labor no es fácil y el único comienzo posible está centrado en un solo concepto: la educación en dos ámbitos: el conductual y el tecnológico. Así, en esta misión los especialistas resaltan como punto de partida una labor conjunta de padres y educadores en estos conceptos.

En el primer aspecto, el **relacionado con la conducta**, hay que tener en cuenta conceptos como:

- Niveles adecuados de comunicación intrafamiliar. Los niveles adecuados de comunicación no se construyen cuando se necesitan, sino que han de estar ya

consolidados para que, cuando sucede algo, pueda sacársele partido, además de las bondades que tienen para la convivencia familiar y la buena relación cotidiana.

- La falta de una concienciación adecuada a las familias, y la capacitación de éstas en habilidades y estrategias que favorezcan esos "niveles adecuados" hace que las familias sean poco eficaces a niveles preventivos.
- Educación en sensibilidad: es importante hacerles comprender el derecho y el respeto a la víctima y ponerse en su lugar para evitar que se llegue a situaciones no solo de violencia, sino también de aislamiento de determinados menores.
- Problemas éticos y pensamiento consecuencial. Resaltar la importancia de enseñar a los niños dos conceptos importantes. Por una parte, en línea con la información que se emite y que se recibe, qué información es creíble y cuál no o qué hay que mantener "en cuarentena", y, cuando somos emisores de información, qué información es publicable y cuál no, desde el punto de vista de la educación, de la importancia de la información, de los riesgos de la información que se comparte e, incluso, de la seguridad física y digital. Y, por otra parte, aprender a analizar las consecuencias de la información que se publica.
- Modelo colaborativo de resolución de problemas entre familias y escuela como forma de abordar los problemas de *ciberbullying* y existencia de un modelo restaurativo de las relaciones interpersonales en la resolución de los casos, frente a la venganza y la Ley de Talión: restitución y restauración.
- No responder a la provocación: desde la Policía se indica que, ante una situación de ciberacoso, es imprescindible no responder a las provocaciones y dejar claro que las acciones del acosador pueden ser constitutivas de delito y que se actuará en consecuencia.

Respecto a la **educación en la tecnología**, las líneas que destacan educadores y técnicos son:

- Educar en el funcionamiento "técnico": hay que darles a conocer los riesgos (virus, spam, suplantación de identidad, etc.), las herramientas que es necesario que estén instaladas en los equipos (antivirus, cortafuegos, etc.), además de los hábitos seguros como el no entrar en páginas que no sean fiables o el uso de contraseñas robustas y su cambio periódico.

- Limitar los horarios de uso para evitar ningún tipo de dependencia a las redes sociales y establecer un lugar de tránsito y uso común para ubicar el ordenador.
- Establecer un criterio de edades, tanto para la utilización de la tecnología como para el acceso a los contenidos.
- Educación familiar y escolar en las que se preserven y eduquen la gestión de los sentimientos y las emociones, la comunicación de los datos personales, el derecho y la salvaguarda de la intimidad y el respeto a la imagen de uno mismo y de los otros.
- Concepto del delito: enseñándoles que las conductas que lleven a cabo en el uso de las nuevas tecnologías y de Internet también pueden tener consecuencias en el ámbito familiar (castigos), en el ámbito escolar (sanciones) o, ya en casos más graves, incluso penales (delitos).

5.1. Prevención del acoso por medio de las TIC.

5.1.1. Cómo prevenir el ciberacoso.

- Piensa, antes de publicar, sobre las consecuencias de compartir esa información.
- Valora la visibilidad que tiene todo aquello que publicamos a través de Internet (WhatsApp, redes sociales, etc.) y su capacidad para hacerse extensivo y quedar fuera de tu control.
- Configura de forma adecuada y personalizada la privacidad de tus redes sociales.
- Protégete. No facilites datos personales.
- Respeta siempre, en tus publicaciones, a los demás y a ti mismo.
- Compórtate con educación y respeto en la Red. Netiqueta.
- Cuida y mantén tus relaciones sociales. Tus amigos son tus mejores aliados a la hora de protegerte.

5.1.2. Cómo actuar ante un caso de ciberacoso.

- No contestes a las provocaciones.
- Si te molestan, abandona la Red.

- Si te acosan, guarda las pruebas.
- Informa o denuncia la situación de acoso a través del administrador del servicio Web (Twitter, Facebook, Instagram, etc.).
- No te sientas culpable. Es quien te acosa quien está cometiendo un delito. Tú no tienes la culpa.
- Pide ayuda siempre a un adulto de referencia y confianza para ti. Si la amenaza es grave, pide ayuda con urgencia.

5.1.3. Otras consideraciones sobre el ciberacoso.

- Comunica lo que piensas de forma asertiva: hablando clara y honestamente sobre tus necesidades, emociones, intereses y opiniones, tomando tus propias decisiones sobre lo que piensas, pidiendo lo que quieres y diciendo "no" a lo que no te gusta o quieres.
- Trata a los demás con amabilidad y respeto.
- No hagas en la Red lo que no harías en persona. Desarrolla tu pensamiento crítico: analiza y cuestiona la realidad, tomando tus propias decisiones.
- Fomenta la empatía en tus relaciones, siendo capaz de ponerte en la piel del otro.
- No callarse ni ocultar el ciberacoso (confiar en familia, profesorado y mediadores). Si detectas o sospechas de una situación de posible acoso a tu alrededor (un/a amigo/a, compañero/a, familiar), no dudes en ofrecerle ayuda, observar qué sucede y reportar el caso a un adulto, que pueda ayudaros a analizar y buscar una posible solución al problema.

5.2. Prevención del ciberacoso con intención sexual.

En el caso del acoso sexual a menores por parte de adultos, o *grooming*, la llegada de los menores a Internet y su presencia en programas de mensajería instantánea, redes sociales, juegos online, etc. ha trasladado el acoso presencial también a la vida virtual. Por esta razón, hay que multiplicar las precauciones no sólo para que el menor haga un buen uso de la red, sino también para que aprende a determinar con qué personas tiene que

relacionarse a través de estos medios y cómo no llevar a cabo acciones como concertar citas con extraños en la vida real o al menos no hacerlo sin la presencia de un adulto.

6. CONSEJOS Y RECOMENDACIONES.

6.1. Consejos para padres, madres y educadores.

Es necesario hacer hincapié en la prevención, y ésta pasa principalmente por inculcar en los menores y adolescentes una cultura de la privacidad. Es decir, conseguir que 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 un ambiente de confianza que facilite que el menor exponga sus ideas y problemas y así reflexione sobre las posibles consecuencias.

Es importante que los padres, madres y educadores sean capaces de trasladar a los menores la confianza suficiente como para que ante una incidencia en la Red, recurran a la opinión experta de un adulto. Existen en Internet numerosos recursos[22] que pueden ser consultados conjuntamente por padres e hijos y que pueden fomentar este clima de confianza.

6.2. Consejos para adolescentes.

El mensaje principal que se debe trasladar a los menores es: *"Cuando envías una información pierdes el control sobre ella y su destino. Piensa antes de publicar"*. Es decir, una vez que se ha decidido pulsar el botón ya no hay marcha atrás y nunca se podrá estar seguro de que la persona a quien se le ha mandado un mensaje, una imagen o un video los mantendrá en la

[22] La pagina web www.pantallasamigas.net es una iniciativa que tiene como misión la promoción del uso seguro y saludable de las nuevas tecnologías y el fomento de la ciudadanía digital responsable en la infancia y la adolescencia.

privacidad. Puede incluso que por error o una acción malintencionada de terceros, esa imagen pase a ser de dominio público.

6.3. Recomendaciones dirigidas a padres y tutores legales.

1. Involucrarse en el uso que los menores hacen de internet. La brecha digital existente entre adultos y niños puede hacer que los padres se mantengan alejados de la realidad virtual en la que viven los menores y adolescentes, para los cuales el uso de las herramientas de la web 2.0 es parte de su vida cotidiana. Esto provoca que, en ocasiones, los padres no consigan comprender las consecuencias que un mal manejo de la tecnología puede tener para sus hijos.
2. Instalar los ordenadores en zonas comunes. Es importante que el ordenador se encuentre en algún sitio común de la casa, permitiendo de esta forma que los padres pueden conocer, en cierto modo, el uso que los menores hacen de la web: utilización de servicios, acceso a determinados contenidos, frecuencia de conexión, duración de las sesiones, etc, sin que esto implique una intromisión en la intimidad del menor.
3. Establecer un horario al uso de Internet y del ordenador. Los menores y adolescentes pasan horas frente al ordenador: una media de 14,5 horas a la semana, según el *Estudio sobre hábitos se seguridad en el uso de las TIC por niños y adolescentes y e-confianza de sus padres* del Observatorio de la Seguridad de la Información de INTECO. Las nuevas tecnologías han cambiado la forma de comunicación entre jóvenes: las redes sociales y plataformas colaborativas son puntos de encuentros públicos y masivos. Los niños se aproximan a Internet de un modo natural. No lo hacen necesariamente con una finalidad, simplemente "están" en Internet, "viven" allí, y lo utilizan para estudiar, charlar o escuchar música. Internet constituye una herramienta básica de relación social y de identidad y, como tal, la presencia de los niños en Internet es una realidad básica e inexorable, y el aprovechamiento que hacen del mismo apoya esta certeza. Asumiendo este aspecto como una realidad, es necesario no obstante determinar unas pautas de utilización claras sobre duración o momento de la conexión, servicios utilizados, etc.

4. Impulsar el uso responsable de la cámara web. Este servicio es una herramienta de comunicación muy utilizada por los usuarios de Internet. Un uso inadecuado puede posibilitar una puerta de entrada para usuarios malintencionados.

   Conviene establecer un control por padres y tutores que garantice información acerca de con qué usuarios y en que ámbito se comunican los menores.

5. Uso de imágenes. Para los menores y adolescentes, las fotografías e imágenes constituyen la principal vía de presentación ante los demás.

   En ese sentido, es fundamental plantearles que no deben enviar fotos ni vídeos personales a ningún desconocido, ya que éste le puede dar un mal uso en la Red.

6. Supervisión. Basta con mantener un control sobre el ordenador o las cuentas de los menores y ver el historial de búsquedas y del navegador. No se trata de que se sientan controlados y coartados: este control debe ser realizado de la forma menos intrusiva posible en su intimidad.

7. Comunicación. Establecer un diálogo permanente con los menores y adolescentes es tarea fundamental de los padres y tutores. La comunicación debe abordar tanto los aspectos positivos del uso de la tecnología como los posibles riesgos que Internet puede implicar. Sólo con un conocimiento riguroso de las situaciones que pueden tener lugar en Internet es posible estar preparado para responder a ellas.

8. Autoprotección. Es necesario plantear a los menores y adolescentes la necesidad de ser cuidadosos con los datos que facilitan en Internet, publican en las redes sociales o proporcionan a través de los servicios de mensajería instantánea. Los niños deben comportarse con responsabilidad, respeto y sentido común en la Red, igual que lo hacen en el mundo físico.

En el caso de ser consciente de la **existencia de alguna de estas conductas**, es recomendable adoptar las siguientes medidas:

- No destruir las evidencias del acoso en cualquiera de sus modalidades (mensajes de texto, correo electrónico, contenidos multimedia, etc.).
- Tratar de identificar al acosador (averiguar su dirección IP, recurrir a especialistas en informática y a las Fuerzas y Cuerpos de Seguridad del Estado).

- Contactar con la compañía del medio empleado para cometer el acoso (compañía de teléfono, propietario del dominio o sitio web, etc.).
- Denunciar el acoso a las Fuerzas y Cuerpos de Seguridad del Estado que disponen de unidades de delitos informáticos.
- En caso de *ciberbullying*, si éste procede del entorno escolar, habrá que tomar tres medidas adicionales:
    - Informar a la escuela, director y al orientador del centro, para recibir el apoyo necesario.
    - Contactar con los padres del agresor.
    - Recurrir a organizaciones especializadas en acoso escolar.

6.4. Recomendaciones dirigidas a los menores.

1. Se recomienda a todos los usuarios recurrir al uso de seudónimos o *nicks* personales con los que operar a través del Internet, permitiéndoles disponer de una auténtica identidad digital que no ponga en entredicho la seguridad de su vida personal y profesional. De esta forma, únicamente será conocido por su círculo de contactos que saben el Nick que emplea en Internet.
2. Ser cuidadoso con los datos personales que se publican. Es recomendable no publicar demasiados datos personales en Internet: redes sociales, plataformas, blogs o foros. Estos datos podrían ser utilizados contra el menor o su entorno.

   Es recomendable no publicar más datos de los necesarios y, en caso de datos como el correo electrónico o teléfono móvil, hacerlo de la forma más privada posible.
3. Se recomienda a los usuarios tener especial cuidado a la hora de publicar contenidos audiovisuales y gráficos, dado que en este caso pueden estar poniendo en riesgo la privacidad e intimidad de personas de su entorno.

   Siempre que se vayan a alojar contenidos de este tipo o información relativa a terceros, se recomienda notificar previamente a ese tercero para que lo autorice o, en su caso, filtre los contenidos que desea publicar y los que no.
4. No aceptar ni agregar como contacto a desconocidos. Es recomendable que el menor se asegure de si la persona que va a agregar es realmente un conocido. Para

asegurarse, en caso de que el nombre de usuario no sea reconocible, puede preguntar a sus contactos si es conocido por ellos (amigos comunes, compañeros de colegio, campamento, vacaciones, etc.). En caso de detectar discrepancias entre el perfil declarado y el real, o si se identifica alguna conducta malintencionada, la mejor opción es bloquear el contacto de forma inmediata. En función de la gravedad de la situación, es recomendable ponerlo en conocimiento de la plataforma y de las autoridades competentes, si se considera necesario.

En estos casos, siempre conviene que lo comunique a sus amigos para que estén prevenidos ante ese contacto.

5. Evitar el envío de imágenes o vídeos a usuarios en los que no se confía. En caso de que un contacto desconocido intente involucrarse de forma muy temprana en nuestra vida social y al poco tiempo solicita que se le envíe una foto o encender nuestra cámara web, es mejor dudar y, en un momento posterior disculparse, que ser afectado de alguna de las conductas mencionadas.
6. Comunicarlo a los padres o tutores. En el momento en que se detecte una situación de riesgo, o en la que un tercero comience a solicitar temas relacionados con aspectos sexuales, se debe comunicar inmediatamente a los padres o tutores legales.

7. APROXIMACIÓN A CASOS REALES CON AMPLIA REPERCUSIÓN MEDIATICA.

7.1. Condena impuesta a J.C.M. por varios delitos de descubrimiento y revelación de secretos. Pornografía Infantil y otros.[23]

VISTO Y OIDO en juicio oral y público ante la Sección Tercera de la Audiencia Provincial de Madrid el Rollo de Sala 58/11 correspondiente a las Diligencias Previas 3986/08 del Juzgado de Instrucción nº 34 de los de Madrid por delito descubrimiento y revelación de secretos, pornografía infantil y otros, contra el acusado JMC, se falló condenar al acusado como responsable en concepto de autor, concurriendo la circunstancia modificativa de la responsabilidad criminal directa analógica de alteración psíquica, de:

- Cincuenta delitos de Descubrimiento y Revelación de Secretos del art. 197.1, 2 y 5 del CP.
- Catorce delitos de Descubrimiento y Revelación de Secretos del art. 197.1 y 2 del CP.
- Nueve delitos de Elaboración de Pornografía Infantil del art. 189.1 a) del CP.
- Un delito contra la integridad moral del art. 173 del CP.
- Tres delitos de amenazas graves del art. 169.1º párrafo primero inciso primero y párrafo segundo del CP.
- Dos delitos de amenazas graves del art. 169.1º párrafo primero inciso segundo y párrafo segundo del CP.
- Un delito de Distribución de Pornografía Infantil del art. 189.1 b) del CP.
- Cinco faltas de injurias del art. 620.2º del CP.

[23] Audiencia Provincial-Madrid, Sección 3ª. Sentencia nº 245/2012. Disponible en: http://www.poderjudicial.es/stfls/TRIBUNALES%20SUPERIORES%20DE%20JUSTICIA/TSJ%20Madrid/NOTAS%20DE%20PRENSA/Sentencia%20Secci%C3%B3n%20Tercera%20AP.%20Caso%20ciberacosador.pdf [consulta: 02/04/2018].

En aplicación de lo dispuesto en el art. 76 CP, se fija como máximo de cumplimiento efectivo de la condena impuesta la de nueve años y veinticuatro meses de prisión.

También se le condena al acusado al pago de las costas procesales, incluidas las de la acusación particular y a las indemnizaciones fijadas en resolución.

En los HECHOS PROBADOS, consta que *el acusado, JMC, sin antecedentes penales, durante los últimos meses del año 2007, a lo largo del año 2008 y los primeros meses del año 2009, valiéndose de sus conocimientos informáticos y ocultando sus datos relativos a sexo y edad, contactaba con personas, casi todas chicas y menores de edad, a través de distintas páginas de internet (votamicuerpo, netlog, sexyono, Messenger o tuenti) y, tras mantener conversaciones, las pedía que le enviasen fotos o videos de ellas desnudas así como les exigía que conectasen la webcam para obtener sus imágenes. Ante la negativa, les profería insultos y amenazas, bloqueándole las cuentas de correo y apoderándose de las mismas, así como de sus contactos, datos personales, fotografías y videos que aquellas tenían en el escritorio o en carpetas de sus ordenadores y no solo de las que las víctimas habían colgado en sus perfiles. Tras ponerle de manifiesto a las victimas el control que tenía sobre sus cuentas y contactos, en muchos de los casos, y que se referirán, consiguió que aquellas les mandasen fotografías y videos mostrando sus cuerpos desnudos, adoptando posturas y actitudes de claro contenido pornográfico, no sin antes amenazarles e insultarles con el fin de obtener una permanencia en el tiempo de dichas conductas.*

A raíz de las denuncias que fueron presentándose por varias víctimas, *la Policía solicitó al Juzgado de Instrucción número 34 de Madrid que oficiara a "Microsoft Corporation" para que informara sobre todos los datos de tráfico de comunicaciones que dispusiera sobre las cuentas xxx y xxx, cuentas desde las que se habían realizado los hechos denunciados. Una vez conocidas las direcciones IP de conexión de las cuentas citadas, el Juzgado dictó sendas resoluciones de fecha 6.8.2008 dirigidas a Telefónica de España S.A.U. y ONO para que informaran del titular de esas direcciones IP en determinadas fechas y horas de conexión. Una vez conocido los dos domicilios desde los que se conectaba el titular de las cuentas, se dictó auto de entrada y registro de fecha 20.10.2008. En la diligencia de entrada y registro de la vivienda sita en la calle xxx de la localidad de xxx se intervino el equipo informático usado por el acusado.*

Pues bien tras el volcado de datos del ordenador y disco duro intervenidos al acusado, se consiguió saber las IP de conexión y las cuentas de correo electrónico de las personas con las que el acusado había mantenido conversaciones a través de Messenger y tras ser localizadas e identificadas prestaron declaración contando lo sucedido, corroborando en la vista oral como tras negarse a facilitarle al acusado fotografías comprometidas o a conectar la webcam tal como les exigía o reprocharle haberle quitado la cuenta de correo a alguna amiga, perdían el control de las mismas, consiguiendo el acusado sus contraseñas y apoderarse de toda la información contenida en dichas cuentas incluso en el escritorio de algunos ordenadores, extremo que los funcionarios de Policía de la BIT pudieron constatar tal como manifiestan en la vista oral.

7.2. Condena impuesta a Gonzalo por un delito de abusos sexuales y varios delitos continuados de exhibicionismo.[24]

La Sección Segunda de la Audiencia Provincial de Tarragona, con fecha ocho de abril de dos mil quince, dictó el siguiente pronunciamiento:

"Que debemos CONDENAR Y CONDENAMOS al acusado Gonzalo a:

1.- Como autor responsable de un delito de abusos sexuales a menor de trece años del artículo 183.1 del Código Penal sin la concurrencia de circunstancias modificativas de la responsabilidad criminal a la pena de…

2.- Como autor responsable de cinco delitos continuados de exhibicionismo del artículo 185 del Código Penal, en relación con el artículo 74 del Código Penal, sin la concurrencia de circunstancias modificativas de la responsabilidad criminal, a la pena de…

3.- A la pena de PROHIBICIÓN de APROXIMARSE a Angelina, Estela, Isidora, Adriana y Modesta a su domicilio, a su lugar de trabajo y cualquier otro que éstas frecuenten, a una distancia inferior de 1.000 metros, durante el tiempo de…

4.- A la pena de PROHIBICIÓN de COMUNICARSE por cualquier medio con Angelina, Estela, Isidora, Adriana y Modesta durante un período de…

5.- En concepto de responsabilidad civil, D. Gonzalo deberá indemnizar por daños morales a Angelina, Estela, Isidora, Adriana y Modesta las siguientes cantidades…

[24] Tribunal Supremo. Sala de lo Penal. STS 5809/2015. Disponible en: http://www.poderjudicial.es/stfls/TRIBUNAL%20SUPREMO/DOCUMENTOS%20DE%20INTER%C3%89S/TSPenal%2010.12.15%20(912-15).pdf [consulta: 05/04/2018].

Que debemos ABSOLVER y ABSOLVEMOS a Gonzalo:

A) Del delito del artículo 183.2 y 3 del Código Penal.

B) Del delito del artículo 183 bis del Código Penal.

Se condena a D. Gonzalo al pago de las costas procesales de este procedimiento en las 6/7 partes. Notifíquese esta Sentencia al condenado, al Ministerio Fiscal y a las partes personadas, haciéndoles saber que contra la misma se puede interponer RECURSO DE CASACIÓN ante la Sala 2ª del Tribunal Supremo, anunciándolo ante este Audiencia Provincial dentro del plazo de cinco días contados a partir del siguiente a la última".

En los HECHOS PROBADOS consta que:

1º.- En fecha no determinada en el año 2012, Gonzalo conoció a la menor Estela, a la cual le envió una petición de amistad a la red social Facebook, la cual fue aceptada por la menor. En la fecha de dicha petición Gonzalo era pleno conocedor de que Estela era menor de edad.

En algunas de dichas conversaciones Gonzalo realizó distintas peticiones a la menor para que mantuviera relaciones sexuales con él. Junto a dichas conversaciones por mensaje de texto, Gonzalo utilizó como medio de comunicación con la menor la webcam de su ordenador, webcam que permitía a la menor ver en su ordenador todo lo que Gonzalo hiciera frente a la cámara de su ordenador. Utilizando dicho sistema de comunicación audiovisual Gonzalo, en tres ocasiones diferenciadas en el tiempo, se desnudó ante su ordenador para que lo viera la menor, una vez desnudo Gonzalo procedió a masturbarse ante ella.

En alguna de dichas conversaciones, la menor Estela le habló a Gonzalo que tenía una amiga, Angelina, también menor de edad, manifestando Gonzalo que la quería conocer. En dichas conversaciones Estela le manifestó que dicha amiga era menor, y que tenía incluso menos años que ella. En dichas conversaciones Gonzalo ya le manifestó a la menor Estela su intención de realizar actuaciones de carácter sexual con dicha menor por lo que debían quedar con Angelina.

2º.- En fecha 27 de octubre de 2012, tras las conversaciones antes indicadas, las menores Estela y Angelina se encontraban en el domicilio de Estela sito…, cuando Gonzalo que se encontraba en su domicilio sito…, a través de la red social Facebook propuso a Estela, de 15 años de edad, quedar al día siguiente para que le realizara una felación delante de Angelina, de 7 años de edad, proponiéndole posteriormente a Angelina que fuera ella quien le realizara la felación. A continuación, movido por la finalidad de satisfacer su impulso sexual, se extrajo su pene y procedió a masturbarse delante de las menores a través de la webcam de su ordenador.

3º.- En fecha 28 de octubre de 2012, Gonzalo se encontró con las menores referidas, Estela y Angelina...

4º.- En el verano del 2012, Gonzalo, mientras se encontraba conversando por escrito con la menor Estela, movido por la finalidad de satisfacer su impulso sexual, tras sacarse el pene, procedió a masturbarse a través de la webcam de su ordenador. De forma súbita entró en la habitación de Estela, su hermana Marí Trini y al ojear el ordenador de Estela, pudo ver a Gonzalo desnudo, cerrando inmediatamente la pantalla Estela.

5º.- Durante el año 2012, Gonzalo contactó por la red social Facebook con Isidora de 16 años de edad, a la que conocía de la escuela, conociendo Gonzalo la minoría de edad de esta. Posteriormente se vieron en diversas ocasiones y en una de ellas Gonzalo procedió a comprar a Isidora ropa interior, tras lo cual le pidió que se la enseñara a lo cual esta no accedió. Posteriormente Gonzalo le pidió que le enviara fotografías en la que mostrara la ropa interior que le había comprado, procediendo la menor a enviarle tres fotografías en las cuales ella se mostraba en ropa interior. Tras enviarle dichas fotos, Gonzalo le pidió en distintas ocasiones para quedar. Tras no acceder a ello la menor, Gonzalo procedió a enviarle al menos dos vídeos en los que aparecía desnudo, masturbándose, e introduciéndose dedos por el ano. Asimismo, pidió a la menor que le enviase fotografías de ella desnuda.

6º.- En fecha indeterminada durante el 2011, Gonzalo en una actuación castellera realizada en fiestas de El Catllar, saludó a la menor Adriana, de 15 años de edad. Posteriormente, tras averiguar su identidad, procedió a enviarle una petición de amistad a la red social Facebook, lo cual fue aceptado por la menor. En la página de facebook de Adriana constaba la fecha de nacimiento de ésta. En el transcurso del tiempo que estuvieron conectados a través de dicha red social, Gonzalo al menos en quince ocasiones procedió a enviar a la menor fotos en las que aparecía desnudo y con el pene erecto. Al menos en cuatro ocasiones, cuando estaban conversando mediante mensajes de texto, Gonzalo procedió a activar la webcam de su ordenador mostrándose ante la menor desnudo y con el pene en erección, y dos de las cuatro, Gonzalo procedió a masturbarse ante la menor.

7º.- Durante el 2010, Gonzalo, contactó a través del Chat Terra con Modesta, de 14 años de edad, minoría de edad de la que era conocedor Gonzalo. En distintas de las conversaciones mantenidas mediante mensajes de texto, Gonzalo realizaba a la menor distintas referencias al sexo, manifestándole su intención de mantener relaciones sexuales con la misma. Gonzalo, cuando la menor tenía entre 14 y 15 años de edad, al menos en diez ocasiones le envió fotografías en las que se mostraba desnudo, con el pene en erección y tocándose. En ese período de tiempo Gonzalo utilizando su webcam, procedió a contactar con la menor, mostrándose desnudo, procediéndose a masturbarse ante la menor al menos en cuatro ocasiones.

Gonzalo, cuando la menor tenía entre los 14 y los 17 años de edad, le pedía a la menor que le enviara fotografías en las que se mostrara desnuda o en ropa interior, logrando con su insistencia hacer nacer en la menor un sentimiento de compromiso ante Gonzalo por lo que ésta le envió al menos cinco fotografías.

8º.- Gonzalo ingresó en prisión en virtud de Auto de fecha 24 de enero de 2013, dictado por el Juzgado de Instrucción n° 1 de Valls y ratificado por Auto de fecha 28 de enero de 2013, dictado por el Juzgado de Instrucción n° 3 de Valls.

Se preparó recurso de casación por infracción de ley y vulneración de precepto constitucional, por el Ministerio Fiscal y el condenado Gonzalo, remitiéndose a la Sala Segunda del Tribunal Supremo las certificaciones necesarias para su sustanciación y resolución, formándose el correspondiente rollo y formalizándose el recurso:

- Motivos aducidos por el Ministerio Fiscal: Infracción de precepto sustantivo del art. 849.1º LECrim por aplicación indebida del art. 8.3 CP, e inaplicación indebida del art. 183 bis (ciberacoso-*child grooming*).

  El fiscal entiende que los delitos de abuso o agresión sexual tipificados en el art. 183 CP no absorben la eventual tipicidad previa del art. 183 bis. Cabría entre ambos una relación de concurso real (en su caso, medial). Discrepa así de la sentencia de instancia que considera que se trata de un concurso de normas penales a solventar con aplicación del art. 8.3 CP (principio de consunción *lex consumens derogat consumpta*): el delito del art. 183 operaría como *lex consumens*.

  Para atacar tal apreciación el Ministerio Publico se apoya en un inciso del art. 183 bis del CP-*"sin perjuicio de las penas correspondientes a los delitos cometidos en su caso"*- que interpreta en clave de concurso real de delitos.

  Sobre estos motivos, la Sala Segunda de lo Penal del Tribunal Supremo falla:

  Que debemos declarar y declaramos NO HABER LUGAR al recurso de casación interpuesto por El Ministerio Fiscal, contra Sentencia y Audiencia arriba reseñadas.

- Motivos aducidos por la representación legal de Gonzalo: Al amparo del art. 852 LECrim por vulneración del art. 18.1 CE referido al derecho a la intimidad del art. 18.3 CE referido al secreto de las comunicaciones y del art. 24.2 CE referido al derecho a un proceso con todas las garantías. Tales vulneraciones derivarían en una

afectación del derecho a un proceso con todas las garantías. Impugna la validez de la prueba consistente en los mensajes tanto de Facebook como de Whatsapp cruzados por el recurrente con las menores. La inutilizabilidad de esa prueba arrastraría la invalidez de las posteriores que traen causa de aquélla.

Tras entrar a examinar pormenorizadamente los miembros del Tribunal los motivos invocados, la Sala Segunda del Tribunal Supremo, falla:

Que debemos declarar y declaramos NO HABER LUGAR al recurso de casación interpuesto por Gonzalo , contra Sentencia dictada por la Sección Segunda de la Audiencia Provincial de Tarragona, que condenó al acusado como autor responsable de un delito de abusos sexuales a menor de trece años, y cinco delitos continuados de exhibicionismo del art. 185 CP. condenándole al pago de las costas ocasionadas en este recurso.

7.3. Condena impuesta a C.T.R. por un delito de distribución de material pornográfico infantil.[25]

En el recurso de amparo núm. 5928-2009, promovido por don C.T.R., representado por el Procurador de los Tribunales don Joaquín Pérez de Rada González de Castejón y asistido por el abogado don Diego Silva Merchante, contra la Sentencia de la Sección Primera de la Audiencia Provincial de Sevilla de 7 de mayo de 2008, dictada en Procedimiento Abreviado núm. 254/2007, que condenó al recurrente como autor de un delito de corrupción de menores a la pena de …, y contra la Sentencia de la Sala de lo Penal del Tribunal Supremo, de 18 de febrero de 2009, dictada en recurso de Casación núm. 1396/2008, que confirmó la condena impuesta.

Los hechos de los que trae causa la demanda de amparo, relevantes para la resolución del caso son, en síntesis, los siguientes:

[25] Tribunal Constitucional. Sala Segunda. Recurso de amparo núm. 5928-2009. Disponible en: http://www.legaltoday.com/informacion-juridica/jurisprudencia/constitucional-y-comunitario/sentencia-num-59282009-tribunal-constitucioanl-07112011. [consulta: 05/04/2018].

a) La Sentencia de la Audiencia Provincial de Sevilla ya referenciada condenó al recurrente como autor de un delito de corrupción de menores del art. 189.1 b) CP a la pena de... Los hechos probados relatan lo siguiente:

"Entre los meses de noviembre y diciembre de 2007, el acusado C. T.R. (mayor de edad y sin antecedentes penales) ha tenido en su ordenador personal portátil numerosos ficheros de fotografías y videos mostrando a menores de edad - muchos de los cuales no alcanzan los trece años - solos o acompañados de otros menores, desnudos en actitudes y prácticas explícitamente sexuales."

Así, en la carpeta "Mis documentos/mis imágenes" el acusado conservaba 17 videos y más de 3.000 fotografías de contenido pedófilo, y en la carpeta "eMule/Incoming" almacenaba más de 140 vídeos y más de 150 fotografías de pornografía infantil.

Los ficheros que representaban tales imágenes fueron obtenidos por el acusado, mediante el sistema de intercambio de archivos en Internet conocido como "Peer to peer", utilizando el mencionado programa eMule, por el que se comparten imágenes mediante su descarga y distribución simultánea. Por este sistema, el acusado -que tenía configurado el programa eMule para poner a disposición de cualquier otro usuario de la red todos los archivos contenidos en el disco duro de su ordenador- distribuyó material pornográfico de menores (muchos de ellos, menores de trece años) en una cantidad equivalente a unos 96 Giga bytes.

Frente a la alegada lesión del derecho a la intimidad, planteada por el recurrente como cuestión previa, la Audiencia Provincial responde lo siguiente:

"Las presentes actuaciones dimanan de la denuncia formulada por el testigo [...] Según la misma - coincidente con su declaración en el plenario-, el acusado se personó en su establecimiento (APP Informática) entregándole su ordenador portátil con el encargo de cambiar la grabadora, que no funcionaba. Una vez efectuada la reparación y para comprobar el correcto funcionamiento de las piezas sustituidas, el testigo - como al parecer es práctica habitual- escogió al azar diversos archivos de gran tamaño (fotografías, videos o música) para grabarlos y reproducirlos en el ordenador, visualizándose entonces las imágenes pornográficas que contenía. El testigo puso entonces tal circunstancia en conocimiento de la Policía Nacional, que procedió a la intervención del portátil y al examen de su contenido, sin solicitar autorización judicial al efecto.

Pues bien, el Tribunal no considera que la actuación de [...] y de la Policía Nacional vulnerara el derecho a la intimidad del inculpado atendiendo a dos razones:

1. El testigo especificó en juicio que, al recibir el encargo, preguntó a don C. T.R. si el ordenador tenía contraseña, a lo que el cliente le respondió que no, sin establecerle limitación alguna en el uso del ordenador y acceso a los ficheros que almacenaba.

En consecuencia, pese a conocer que el técnico accedería al disco duro del ordenador (pues para ello le solicitó la contraseña), el acusado consintió en ello sin objetar nada ni realizar ninguna otra prevención o reserva que permita concluir que pretendía mantener al margen del conocimiento ajeno determinada información, datos o archivos.

2. En ello abunda precisamente el hecho de que, como señaló el perito funcionario policial núm. 101.182 corroborando así la conclusión del informe pericial documentado, el acusado tenía configurado el programa eMule de manera que todos los archivos del disco estuvieran a disposición de cualquier otro usuario de la aplicación.

En definitiva, difícilmente puede invocarse el derecho a la intimidad cuando los propios actos del acusado indican paladinamente que no tenía intención ni voluntad alguna de preservar para su esfera íntima, exclusiva y personal ninguno de los ficheros que conservaba en su ordenador, pues a ellos tenía acceso cualquier persona que se conectara en Internet a la misma red de intercambio".

b) La Sentencia del Tribunal Supremo desestimó el recurso de casación interpuesto.

En definitiva, ha de concluirse que la condena del demandante como autor de un delito de distribución de material pornográfico infantil del art. 189.1 b) CP se sustenta en pruebas de cargo válidamente practicadas, al haberse acomodado a las exigencias constitucionales, mediante un razonamiento debidamente explicitado en las resoluciones judiciales, como hemos comprobado, que no puede calificarse de irrazonable, puesto que los datos tenidos en cuenta resultan suficientemente concluyentes, sin que a este Tribunal le competa realizar ningún otro juicio ni entrar a examinar otras inferencias propuestas por quien solicita el amparo.

En atención a todo lo expuesto, el Tribunal Constitucional, POR LA AUTORIDAD QUE LE CONFIERE LA CONSTITUCIÓN DE LA NACIÓN ESPAÑOLA, ha decidido:

Desestimar la demanda de amparo presentada por don C. T.R.

8. CONCLUSIONES.

La revolución de las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del cibercrimen, no ha terminado todavía ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas.

Hoy, la utilización de los servicios de Internet o las redes de la telefonía móvil constituyen la forma más común de comunicarse personalmente con familiares, amigos o personas del entorno laboral, y no sólo para adultos sino también para los menores de una generación que no entenderá la comunicación entre iguales sin la Red. Además, todo parece indicar que la incidencia del ciberespacio en todos los aspectos de la vida social no va a ir disminuyendo, sino que seguirá creciendo. Conforme lideren el mundo los denominados "nativos digitales" o nacidos en la era de la web 2.0 popularizada, con los sistemas informáticos como forma de trabajo y también de diversión, con las redes sociales como forma de interactuación social, con las tecnologías móviles totalmente conectadas y con toda la información en la palma de su mano, el ciberespacio, como lugar de encuentro por el uso de las TIC, irá expandiéndose y la novedad del cibercrimen, como de cualquier otro elemento concatenado a ese espacio virtual que es para muchas personas aún más real que el otro, irá desapareciendo y lo único que cambiará será la concreta manifestación de éste a raíz del nuevo aspecto social digno de protección o la nueva tecnología que facilitará o modificará la forma de la comisión del delito.

El presente trabajo aborda el análisis de la respuesta del Código penal a las distintas variedades de acoso a menores realizados en el ciberespacio. Los menores, por tanto,

pueden sufrir, por parte de compañeros o de adultos, una amplia gama de ataques que pueden afectar a su honor, intimidad, libertad o dignidad.

La jurisprudencia ha reconducido a distintos tipos penales muchas de las conductas que, con poca precisión, podríamos denominar de "acoso a menores a través de Internet". Y lo ha hecho, como no podría ser de otra forma, a partir de los distintos bienes jurídicos de los menores dañados o puestos en riesgo por los distintos ciberataques. El honor, la libertad, la intimidad, entre otros bienes de los menores que pueden ser afectados, delimitarán la concreta respuesta jurídica.

Ante las situaciones de riesgo descritas a lo largo del trabajo, el papel que juegan los padres o tutores de los menores es crucial. Éstos, con independencia de controlar y establecer medidas y normas de uso en Internet, deben ser conscientes de que pueden actuar con inmediatez en dos líneas prioritarias:

- En primer lugar, procurar la seguridad del menor, evitando que continúe manteniendo cualquier tipo de relación con el acosador.
- En segundo lugar, denunciar los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado, que darán traslado a los grupos especializados en delitos informáticos para que sea investigado el caso en cuestión.

El principal consejo a los padres es que sean el mejor ejemplo para sus hijos, también en Internet. Si nuestro hijo ve que ponemos una foto sexy hará lo mismo. Si ve que cuidamos nuestra reputación digital también lo hará él y se evitará problemas en un futuro. Lo ideal sería crear entornos TIC seguros adaptados a cada edad y cada momento de madurez. No funciona fiscalizar las actividades de los hijos: se trata de ofrecerle recursos y pensamiento crítico frente a los posibles riesgos de la red. Explicarle qué son los ajustes de privacidad, cómo sospechar de perfiles falsos, cómo tapar la webcam, por qué no podemos fiarnos de correos electrónicos que nos piden contraseñas y datos bancarios ni subir fotos donde aparezcan menores a las redes sociales.

BIBLIOGRAFIA

- ✓ AGUSTINA SANLLEHI, JR. (2017). "La protección penal de la propia imagen: las redes sociales como nuevo entorno y sus implicaciones jurídicas", en *Món jurídic: butlletí del Col.legi d'Advocats de Barcelona,* núm. 312, p. 30-32.
- ✓ AGUSTINA SANLLEHI, JR. (2013). "Victimización en el ciberespacio. Consideraciones victimológicas y victimodogmáticas en el uso de las TIC", en *prensa.*
- ✓ AGUSTINA SANLLEHI, JR. (2011). "¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el Sexting", en *Revista Electrónica de Ciencia Penal y Criminología,* núm. 12-11, p. 11:1-11:44.
- ✓ BARRERA IBAÑEZ, S. (2013). "Investigación criminal de los delitos cometidos contra menores como usuarios de internet", en Pérez Álvarez, S., Burguera Ameave, L., Paul Larrañaga, K. *Menores e Internet*, Aranzadi, p. 407-432.
- ✓ CALMAESTRA VILLEN, J. (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto*. Tesis doctoral. Córdoba: Servicio de Publicaciones de la Universidad de Córdoba, http://helvia.uco.es/handle/10396/5717 [consulta: 10/04/2018].
- ✓ CAMPOS FREIRE, F. (2008). "Las redes sociales trastocan los modelos de los medios de comunicación tradicionales", en *Revista Latina de Comunicación Social*, 63, p. 287-293.
- ✓ GARCIA GUILABERT, N. (2014). *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio*. Tesis Doctoral. Murcia: Servicio de Publicaciones de la Universidad de Murcia, http://hdl.handle.net/10201/40868 [consulta: 10/04/2018].
- ✓ GARCIA GUILABERT, N. (2016). "Actividades cotidianas de los jóvenes en Internet y victimización por malware", en *Revista de los Estudios de Derecho y Ciencia Política*, núm. 22, p. 59-62.
- ✓ GARCÍA MARTIN, I. (2013). "Aspectos psicológicos de la influencia de internet en el libre desarrollo de la personalidad del menor", en Pérez Álvarez, S., Burguera Ameave, L., Paul Larrañaga, K. *Menores e Internet*, Aranzadi, p. 81-109.

- ✓ MARCO MARCO, J.J. (2010). "Menores, ciberacoso y derechos de la personalidad", en García González, J. *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch, p. 85-107.
- ✓ MIRO LLINARES, F. (2011). "La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen", en *Revista Electrónica de Ciencia Penal y Criminología,* 13-07, p. 1-50.
- ✓ MIRO LLINARES, F. (2012). "El Ciberacoso", en Miró Llinares, F., Felson, M. *El Cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons Ediciones Jurídicas y Sociales, S.A., p. 84-99.
- ✓ MIRO LLINARES, F. (2013). "Derecho penal, cyberbullying y otras formas de acoso (no sexual) en el ciberespacio", en *Revista de los Estudios de Derecho y Ciencia Política*, núm. 16, p. 61-75.
- ✓ PARDO ALBIACH, J. (2010). "Ciberacoso: cyberbullyng, grooming, redes sociales y otros peligros", en García González, J. *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch, p. 51-85.
- ✓ PRENSKY, M. (2001). "Digital Natives, Digital Immigrants", en *On the Horizon.* MCB University Press, Volumen 9, Núm. 5.
- ✓ ROBLES, J.M., TORRES ALBERO, C., MOLINA MOLINA, O. (2010). "La brecha digital: un análisis de las desigualdades tecnológicas en España", en *Revista de ciencias sociales,* núm. 218, p. 3-22.
- ✓ RODRIGUEZ NUÑEZ, A. (2013). "Protección penal de los derechos fundamentales de los menores usuarios de internet" en Pérez Álvarez, S., Burguera Ameave, L., Paul Larrañaga, K. *Menores e Internet*, Aranzadi, p. 367-406.
- ✓ SAVE THE CHILDREN (2010). La tecnología en la preadolescencia y adolescencia: Usos, riesgos propuestas desde los y las protagonistas.
- ✓ WALL, DS. (2007). *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge*, UK;* Malden*, MA USA:* Polity Press.
- ✓ YUCEDAL, B. (2010). *Victimization in Cyberspace: An Application of Routine Activity and Lifestyle Exposure Theories*. Tesis doctoral. Kent: Universidad Estatal de Kent. https://etd.ohiolink.edu/!etd.send_file?accession=kent1279290984&disposition=inline [consulta: 10/04/2018].

WEBS DE INTERES

- https://www.is4k.es
- http://xuventude.xunta.es/uploads/Gua_de_actuacin_contra_el_ciberacoso.pdf
- https://www.educacion.navarra.es/documents/57308/57740/ciberbullyng.pdf/1c169fb5-b8ab-478f-b7f4-7e3d22adab14
- https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf
- http://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf
- http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf
- http://www.proteccionline.com/los-riesgos-en-internet-ciberacoso-grooming-sexting-pornografia

ENLACES DE VIDEOS RELACIONADOS

CIBERACOSO y CIBERBULLYING

- https://www.youtube.com/watch?v=zRjRWMwtXVs (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 1/6)
- https://www.youtube.com/watch?v=myz1zuhwKpY (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 2/6)
- https://www.youtube.com/watch?v=7K_Pg0_JEpM (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 3/6)
- https://www.youtube.com/watch?v=HtZTDezlpk4 (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 4/6)
- https://www.youtube.com/watch?v=gvb75Jk54Wg (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 5/6)
- https://www.youtube.com/watch?v=bryW8QoasYs (Seis recomendaciones para la prevención del Ciberbullying Pantallas Amigas 6/6)
- https://www.youtube.com/watch?v=SEC_dOWFN5M (Ciberbullying: ciberacoso en redes sociales, videogames, smartphones... y su prevención Pantallas Amigas)
- https://www.youtube.com/watch?v=tVAjiyNzYq0 (¿Cómo actuar ante el ciberacoso? Ignora, bloquea, pide ayuda y denuncia Pantallas Amigas)

SEXTING y SEXTORSION

- ✓ https://www.youtube.com/watch?v=Oi-VacTFPQA (¿SEXTING? Piénsalo: existe otra persona implicada de quien ahora dependes (1/10))
- ✓ https://www.youtube.com/watch?v=IMQ9sBDi91s (¿SEXTING? Piénsalo: las personas y las relaciones pueden cambiar (2/10))
- ✓ https://www.youtube.com/watch?v=XFUxUtwgkVU (¿SEXTING? Piénsalo: la protección de la información digital es complicada (3/10))
- ✓ https://www.youtube.com/watch?v=fnY8eyY7bNA (¿SEXTING? Piénsalo: la distribución de información digital es incontrolable (4/10))
- ✓ https://www.youtube.com/watch?v=bXQ9P4JJwn0 (¿SEXTING? Piénsalo: una imagen puede aportar mucha información (5/10))
- ✓ https://www.youtube.com/watch?v=vp0VhFCjOQY (¿SEXTING? Piénsalo: existen leyes que penalizan acciones ligadas al *sexting* (6/10))
- ✓ https://www.youtube.com/watch?v=dtzk41Eo9gc (¿SEXTING? Piénsalo: se produce sextorsión si la imagen cae en manos de chantajistas (7/10))
- ✓ https://www.youtube.com/watch?v=Ug4A9tG-4wg (¿SEXTING? Piénsalo: Internet es rápida y potente (8/10))
- ✓ https://www.youtube.com/watch?v=MeXkBoAZjZI (¿SEXTING? Piénsalo: las redes sociales facilitan la información a las personas cercanas (9/10))
- ✓ https://www.youtube.com/watch?v=Hy9UuNNQZzk (¿SEXTING? Piénsalo: existe riesgo de *ciberbullying* si la imagen se hace pública en Internet (10/10))
- ✓ https://www.youtube.com/watch?list=PLUGAcyUkQe0qLW6UARPMKIU6SlXl8t4L&v=H_v0v70WFaA (Sextorsión, una forma de violencia sexual digital)

LISTADO DE ACRONIMOS

AEPD: Agencia Española de Protección de Datos.

AP: Audiencia Provincial.

BIT: Brigada de Investigación Tecnológica de la Policía Nacional.

BOE: Boletín Oficial del Estado.

CE: Constitución Española.

CNI: Centro Nacional de Inteligencia.

CP: Código Penal.

FCSE: Fuerzas y Cuerpos de Seguridad del Estado.

GSM: (*Global System for Mobile*). Sistema Global para las comunicaciones móviles.

IMEI: (*International Mobile Equipment Identity*).
Identidad Internacional de Equipo Móvil.

IMSI: (*International Mobile Suscriber Identity*).
Identidad Internacional del Abonado a un Móvil.

INTECO: Instituto Nacional de Tecnología de la Comunicación.

IP: (*Internet Protocol*). Protocolo Internet.

LECrim: Ley de Enjuiciamiento Criminal.

LO: Ley Orgánica.

LOFCS: Ley Orgánica de Fuerzas y Cuerpos de Seguridad.

LOPD: Ley Orgánica de Protección de Datos de carácter personal.

LOPJ: Ley Orgánica del Poder Judicial.

LOPJM: Ley Orgánica de Protección Jurídica del Menor.

LORPM: Ley Orgánica de Responsabilidad Penal del Menor.

MSISDN: (*Mobile Station Integrated Services Digital Network*).
Estación Móvil de la Red Digital de Servicios Integrados.

PDA: (*Personal Digital Assistant*). Asistente Digital Personal.

RD: Real Decreto.

RDSI: Red Digital de Servicios Integrados.

SIM: (*Subscriber Identity Module*). Módulo de Identificación de Suscripción.

STC: Sentencia del Tribunal Constitucional.

STS: Sentencia del Tribunal Supremo.

TC: Tribunal Constitucional.

TCP: Protocolo de Control de Transmisión.

TIC: Tecnología de la Información y la Comunicación.

TS: Tribunal Supremo.

UE: Unión Europea.

UIT: Unión Internacional de Telecomunicaciones.

UMTS: (*Universal Mobile Telecommunications System*).
Sistema Universal de Telecomunicaciones Móviles.

USA: (*United States of American*). Estados Unidos de América.