



UNIVERSIDAD DE ALMERÍA
FACULTAD DE CIENCIAS SOCIALES Y JURÍDICAS

TRABAJO FIN DE GRADO

LOS ATAQUES INFORMÁTICOS A LA INTIMIDAD SEXUAL: EL SEXTING Y EL DERECHO AL OLVIDO

COMPUTER ATTACKS ON SEXUAL PRIVACY: SEXTING AND THE RIGHT TO BE FORGOTTEN

RESUMEN: Las tecnologías de la información y la comunicación se encuentran en un desarrollo vertiginoso. Aquí surge el *Sexting*, un fenómeno que se caracteriza por la divulgación de imágenes o vídeos de contenido sexual a través de las redes sociales y móviles, sin autorización del afectado. Esta utilización doméstica y privada de la informática pone en relieve la importancia de relacionar el derecho al olvido con otra serie de derechos constitucionales como el derecho a la intimidad.

ABSTRACT: Information and communication technologies are developing at a dizzying pace. This is the origin of Sexting, a phenomenon characterized by the dissemination of images or videos of sexual content through social networks and cell phones, without the authorization of the person concerned. This domestic and private use of information technology highlights the importance of linking the right to be forgotten with other constitutional rights such as the right to privacy.

AUTORA: MARÍA JOSÉ ASENSIO FIGUEROA

TUTORA: MARÍA DOLORES MACHADO RUIZ

GRADO EN DERECHO

CONVOCATORIA EXTRAORDINARIA JULIO 2021



ÍNDICE

I.INTRODUCCIÓN.....	pág. 3
II. PUNTO DE PARTIDA: LOS CIBERDELITOS.....	pág. 4
2.1 Ciberespacio y ciberdelitos.....	pág. 5
2.2 Una modalidad de ciberdelitos: el <i>Sexting</i>	pág. 7
III. LA INCORPORACIÓN DEL SEXTING EN NUESTRO SISTEMA PENAL.....	pág. 9
3.1 Requisitos típicos.....	pág. 10
3.2 Modalidades agravadas.....	pág. 15
IV. NUEVAS INICIATIVAS DE PROTECCIÓN PARA LAS VÍCTIMAS DE CIBERDELITOS: EL DERECHO AL OLVIDO DIGITAL.....	pág.17
4.1 ¿Qué es el olvido digital?.....	pág.18
4.2 La consagración del derecho al olvido en la Unión Europea: especial referencia al caso español.....	pág.22
V. APLICACIÓN JUDICIAL DEL OLVIDO DIGITAL EN NUESTRO PAÍS...pág.26	
VI. CONCLUSIONES.....	pág.30
VII.BIBLIOGRAFIA.....	pág.31

I. INTRODUCCIÓN

Hoy en día nos encontramos ante un mundo completamente digitalizado donde las Tecnologías de la Información y la Comunicación (TIC) han conseguido tener un papel de vital importancia en cualquier aspecto de nuestra vida. Este desarrollo ha alcanzado tal magnitud que ha dado lugar a la aparición de nuevos fenómenos delictivos para la sociedad, a la vez que ha influido en la realización de fenómenos delictivos ya existentes.

Uno de los ámbitos donde más han irrumpido estas tecnologías es la manera de socializarse de las personas, la denominada “generación de internet”; que hace referencia a aquellas personas que han nacido rodeadas de esas nuevas tecnologías. El consecuente incremento del uso de las redes sociales para comunicar y relacionarse ha provocado un cambio en la percepción social de la intimidad y de lo que tradicionalmente se reservaba al ámbito de lo privado. Muestra de ello, es que con solo abrir aplicaciones como *Facebook* o *Instagram* podemos observar cómo las personas les gusta compartir prácticamente su día a día, desde lo qué comen hasta los aspectos más íntimos de su vida privada.

En este contexto, el ámbito de la vida sexual de las personas es uno de los aspectos que más se ha visto afectado por esta evolución tecnológica. Así sucede particularmente en el caso de menores que, además de tratarse de un grupo vulnerable que se encuentra en una etapa de formación sexual, su empleo generalizado de las nuevas tecnologías no les hace conscientes de los peligros que supone las amplias posibilidades de comunicación y difusión que ofrecen estos medios.

Este interesante y complejo panorama me ha llevado a elegir el *Sexting*, como objeto de este trabajo. Los motivos son varios, desde el especial interés que despiertan estos delitos de reciente creación realizados a través de medios informáticos, la dificultad que presenta su persecución práctica hasta el alto riesgo que puede representar el empleo de esas redes sociales o de Internet para los intereses más personales de sus víctimas. Así sucedió en el caso de la concejala Olvido Hormigos, primer supuesto de *Sexting* en España, donde se difundió por su expareja escenas íntimas de contenido sexual en contra de su voluntad. Otra muestra de las graves consecuencias que este fenómeno representa para sus víctimas es el

caso de “La manada”, donde la víctima vio dañada no solo su libertad sexual, sino también su intimidad mediante la posterior difusión por el móvil de ese atentado sexual grupal, propiciando que toda España presenciara en primera fila todas las aberraciones sexuales de las que fue objeto, con el consecuente perjuicio a su reputación social y personal.

Surge así la necesidad de establecer una respuesta penal para hacer frente a esta nueva forma de criminalidad y conseguir una efectiva protección de los bienes jurídicos afectados como la intimidad o el honor, entre otros. Si bien, parece conveniente antes de entrar en su estudio valorar el contexto donde se produce, el ciberespacio, junto a las particularidades que presentan los delitos cometidos dentro de él, los ciberdelitos. Posteriormente, se procederá a exponer los motivos que llevaron a su incorporación en nuestro texto punitivo, así como explicar en qué consiste el Sexting, sus requisitos y las diversas modalidades que presenta. Finalmente, es necesario aludir a unas de las nuevas medidas de protección más eficaces para las víctimas de ciberdelitos, el derecho al olvido. Se valorará el respaldo legal que ha recibido esta medida por la Unión Europea, así como su repercusión práctica por parte de nuestros tribunales.

II. PUNTO DE PARTIDA: LOS CIBERDELITOS

Se puede afirmar que el origen de Internet surgió con el *Advanced Research Projects Agency Network* (ARPANET), que consistía en una red creada por el departamento de defensa de EEUU para comunicarse entre los distintos organismos gubernamentales. Desde entonces hasta ahora ha evolucionado de manera muy rápida creando una vía de comunicación virtual sin precedentes, que se ha extendido a todos los ámbitos de la vida: instituciones públicas, empresas y, sobre todo, entre los particulares.

Uno de los avances más revolucionarios que nos ha proporcionado ha sido la facilidad de acceso y distribución de información. A cambio esta herramienta se ha convertido en un medio eficaz de comisión de delitos, entre los que cabe destacar los atentados a los bienes jurídicos más íntimos de las personas. De este modo, la delincuencia ha encontrado una nueva forma de ataque más eficaz y difícil de perseguir en un sistema social globalizado y digital como el existente en nuestros días, transformando tanto algunos ilícitos tradicionales como creando otros nuevos, dando lugar a lo que hoy se denomina “ciberdelitos”. Veamos en qué consisten y las peculiaridades que presentan.

2.1. Ciberespacio y ciberdelitos

La aparición de internet ha sido uno de los mayores inventos del siglo XX que ha alterado nuestra sociedad de una manera única. Desde el momento que cualquier quehacer de la vida diaria se ha visto trasladado al ciberespacio. De hecho, las TIC se han implantado en todos los ámbitos de nuestras vidas personal y laboral permitiendo poder comunicarnos con cualquier persona del mundo a través de las redes sociales, a la vez que otras puedan acceder y controlar nuestros datos más privados como los bancarios o sanitarios. Un buen ejemplo ha sido este último año como consecuencia de la situación provocada por el COVID-19, donde estos sistemas han adquirido un gran protagonismo debido a la cuarentena y a la necesidad de recurrir al teletrabajo en la mayoría de los sectores laborales a nivel mundial.

Nadie cuestiona que son muchos los avances que nos aportan las nuevas TIC para un mejor desenvolvimiento social, ya que el ciberespacio elimina cualquier frontera física permitiendo a cualquier usuario acceder y conectarse entre sí a nivel global. Pero también el uso irresponsable de las TIC genera serios peligros para sus usuarios, ya que posibilita la comisión de delitos desde cualquier lugar afectando a personas por todo el mundo. De este modo surge una delincuencia deslocalizada que exige la cooperación internacional entre los países para lograr su efectiva persecución y castigo. Tengan en cuenta que estamos ante una herramienta que otorga cierto anonimato que dificulta la identificación de la persona real que hay detrás del perfil *online*. Así lo apuntaba ya ROMEO CASANOBA al señalar que “aunque pudiera seguirse el rastro digital dejado al iniciar la comunicación y proseguir la navegación y accesos correspondientes, hasta conocer desde que terminal y a través de que servidor se operó en la red, no es tan fácil identificar el individuo concreto que realmente fue el que lo perpetró”¹.

Precisamente esa facilidad de transmisión de datos a nivel internacional explica que los daños que puede causar un ilícito en este marco sean mucho mayores que si se realizase de manera convencional. Por ejemplo, un delito de calumnias no provoca el mismo daño si solo se propaga en el pueblo de la víctima que si se difunde a través de las redes sociales a

¹ Cfr. ROMEO CASABONA, C.M (2006): “De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal”, en *El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales*. Editorial Comares, Granada, p.3.

cualquier persona y lugar. No es de extrañar que esa potencialidad lesiva y la impunidad que comporta este espacio virtual haya sido aprovechada por la criminalidad organizada para la comisión de delitos a nivel mundial con total impunidad.

De ahí que una de las primeras cuestiones a analizar sea determinar qué debe entenderse por ciberespacio. Entre sus primeras definiciones, destaca la propuesta por La Comisión Europea como “el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo”. Una definición que no tardó mucho en ser ampliada debido al crecimiento imparable de Internet como “un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas”; que se caracteriza “por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada”².

Tales características comportan una mayor dificultad en la persecución de los delitos cometidos en este ámbito que obliga a adoptar soluciones jurídicas materiales y procesales adecuadas para hacer frente a esta nueva oportunidad criminal. Así lo muestran diversos estudios sobre la materia donde destacan el enorme coste que provoca la ciberdelincuencia en la economía nacional e internacional, convirtiendo esta modalidad delictiva en un negocio más rentable que el tradicional tráfico de drogas³.

Surgen así lo que hoy denominamos ciberdelitos. Su análisis es tan complejo que hasta su simple denominación ha sido controvertida por la diversidad de términos empleados para definir esos delitos cometidos en la red: ciberdelincuencia, delitos telemáticos, etc. La doctrina se encuentra dividida entre calificarlos como “delitos informáticos” o “ciberdelitos”. El primer término surge al expandirse el uso de Internet, aunque son pocos los que siguen empleando los delitos informáticos para referirse a esta nueva clase de criminalidad. La razón de su empleo es que entienden que no se trata tanto de una categoría delictiva como de un nuevo ámbito para la realización de delitos tradicionales que deben

² Cfr. MARTINEZ ATIENZA, G. /BERMEJO FERNÁNDEZ, D. (2020): *Ciberdelitos*, Ediciones Experiencia, pp. 17-18.

³ En ese sentido, ANGUITA OSUNA, J.E. (2018): “Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea”. *Revista de Estudios de Seguridad Internacional*. Vol. 4, núm. 1, pp. 107-126. Disponible en: <https://seguridadinternacional.es/resi/html/analisis-historico-juridico-de-la-lucha-contra-la-ciberdelincuencia-en-la-union-europea/>

adaptarse a las exigencias de la sociedad digital. Es el caso de DAVARA RODRÍGUEZ que lo define como aquel que “reuniendo las características que delimitan el concepto de delito es llevado a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático”⁴. Se refiere, por ejemplo, a quien utiliza las redes sociales para vigilar telemáticamente los movimientos de sus víctimas para robarles cuando están ausentes. Mientras que el término “ciberdelito” cuenta hoy con más respaldo doctrinal y de la jurisprudencia⁵, así como por la legislación internacional sobre la materia como el Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001, celebrado en Budapest. Este concepto englobaría a todas las figuras delictivas que requieren el uso de las TIC como medio imprescindible y expresamente tipificado para su comisión como la estafa informática que, mediante el acceso ilícito a las claves bancarias de una persona, logra disponer de su dinero como si fuera su titular.

Se puede concluir entonces que el término ciberdelito es el concepto más adecuado para designar a estos delitos que operan a través de Internet y las TIC, ya que tales medios no solo señalan el marco virtual donde se desarrollan, sino que además se configuran como los medios típicos para llevarlos a cabo.

2.2 Una modalidad de ciberdelitos: el *Sexting*

El origen etimológico del *Sexting* se encuentra en la unión de dos palabras de procedencia anglosajona: *sex* (sexo) y *text* (envío de mensajes de texto), que traducido al español significa sextear. En 2005 surge en los países anglosajones para denominar el envío de mensajes de textos con carácter sexual. Actualmente, su significado se ha ampliado a causa del desarrollo de las nuevas tecnologías como los *smartphones* y el surgimiento de nuevas redes sociales como *WhatsApp*, que facilitan la comunicación mediante imágenes o videos de manera instantánea.

Según el Observatorio de la Seguridad de la Información, el *Sexting* consiste en “la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual,

⁴ Cfr. DAVARA RODRIGUEZ, M. (1993): *Derecho informático*. Editorial Aranzadi, Madrid, p. 302.

⁵ Así lo califica la Sentencia del Tribunal Supremo 70/2020, de 27 de febrero, que condena con una multa de 1080€ a un hombre que reenvió desde su teléfono móvil una imagen que le había enviado una amiga suya, en la cual aparecía desnuda y sin el consentimiento de esta, a su pareja sentimental.

producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico”. El contenido de carácter sexual generado de manera voluntaria por su autor “pasa a manos de otra u otras personas, pudiendo entrar en un proceso de reenvío masivo multiplicándose su difusión”⁶.

Si bien, esta práctica puede realizarla cualquier persona que disponga de un teléfono móvil con acceso a Internet, llama la atención que esta está más extendida entre jóvenes y menores de edad. La razón, según el estudio realizado por AGUSTINA/GÓMEZ DURÁN, se encuentra en “la revolución sexual que ha acompañado a la revolución tecnológica. En un contexto de hipersexualidad, marcado por el deseo de explorar la sexualidad, los jóvenes, desinhibidos por las propias características coyunturales de la red, adoptan conductas de riesgo que no ejecutarían en el escenario de las relaciones y contactos cotidianos”⁷. Lo que tiene sentido, si tenemos en cuenta que los jóvenes pertenecen a esta era tecnológica donde no solo les proporciona posibilidad de comunicarse fácilmente, sino que además no tienen cultura de privacidad porque todos comparten su vida mediante las redes sociales. Por ello, tienden a normalizar más esta práctica sin llegar a ser conscientes del riesgo que puede suponer la difusión de estas imágenes que afectan tanto a su intimidad personal. Incluso en el caso de los menores de edad exige un tratamiento jurídico especial, en tanto que al ser imágenes de contenido sexual su difusión puede tipificarse como distribución de pornografía infantil.

En cualquier caso, es incuestionable que este tipo de prácticas tan extendidas en nuestros días son lo suficientemente graves para justificar la intervención penal para lograr su prevención y castigo.

⁶ Cfr. PÉREZ SAN JOSÉ, P. (2011) *Guía sobre adolescencia y Sexting: qué es y cómo prevenirlo*. INTENCO, p.4. Disponible en: <https://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf>

⁷ Cfr. AGUSTINA, J. R./GÓMEZ-DURÁN, E. L. (2016): “Factores de riesgo asociados al Sexting como umbral de diversas formas de victimización. Estudio de factores correlacionados con el Sexting en una muestra universitaria”, *Revista de Internet, Derecho y Política*, núm. 22; pp. 32-58. Disponible en: <https://www.raco.cat/index.php/IDP/article/view/n22-agustina-gomez/408480>

III. LA INCORPORACIÓN DEL SEXTING EN NUESTRO SISTEMA PENAL

El Código Penal de 1995 en su redacción original tutelaba el derecho a la intimidad mediante el art. 197, donde se tipificaba como delito únicamente la obtención de imágenes sin el consentimiento del titular. Ante las nuevas necesidades que incorpora la sociedad digitalizada este precepto quedó muy limitado. En 2012 empieza a debatirse la necesidad de incriminar determinados atentados contra la intimidad mediante Internet que carecían de protección jurídica. Concretamente, la difusión no autorizada de imágenes de contenido sexual consentidas anteriormente por la víctima, a pesar de que dañaban gravemente el derecho a su intimidad.

La alerta social sobre tales comportamientos virtuales contra la intimidad se generó a partir de dos casos muy mediáticos sucedidos en Canadá y España. El primero fue el de Amanda Todd, una joven canadiense que sufrió *bullying* por parte de sus compañeros después de que un amigo enviase a todos sus conocidos una imagen suya en *topless*. Después de años viviendo en una pesadilla constante, la joven subió a *YouTube* un vídeo en el que mediante tarjetas contó su historia y poco después se suicidó. Este video acabó siendo viral y hoy en día cuenta con más de 14 millones de visualizaciones. El segundo fue el caso español de la concejala Olvido Hormigos, donde la pareja con la que tenía una relación extramatrimonial difundió un video sexual que ella misma había grabado para él, dando eco de ello todos los medios de comunicación. A pesar de que este hecho llegó a los tribunales quedó impune, ya que en ese momento no se le podía imputar ningún delito al obtenerse las imágenes con el consentimiento de la víctima. Como se indicaba en el Auto, “sólo si se hubiera producido un acceso no autorizado al móvil de la propia denunciante donde se encontraba registrado y grabado el vídeo de contenido íntimo, se entendería consumado el tipo penal”⁸.

Ante este vacío legal, el legislador decidió dar respuesta penal a estos atentados mediante la incorporación del *Sexting* a nuestro texto punitivo a través de la reforma operada por la Ley Orgánica 1/2015 de 30 de marzo. La propia Exposición de Motivos justifica su introducción, alegando que “los supuestos a los que ahora se ofrece respuesta son aquellos otros en los que las imágenes o grabaciones de otra persona se obtienen con su

⁸ Auto del Juzgado de Primera Instancia e Instrucción núm. 1 de Orgaz de 15 de marzo de 2013.

consentimiento, pero son luego divulgados contra su voluntad, cuando la imagen o grabación se haya producido en un ámbito personal y su difusión, sin el consentimiento de la persona afectada, lesione gravemente su intimidad”.

3.1 Requisitos típicos

El delito de *Sexting* se encuentra ubicado en el Título X del Código Penal donde se regulan los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. El derecho a la intimidad es un derecho fundamental consagrado en el art. 18 de la Constitución Española (en adelante, CE). Como bien señala ALCALÉ SÁNCHEZ, se trata de “un derecho personalísimo, irrenunciable, disponible por su titular y que deriva directamente de la dignidad de la persona”⁹.

El tipo básico se regula en el art. 197.7 del Código Penal (en adelante, CP) que estipula:

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

Atendiendo a la definición mencionada, puede destacarse la concurrencia de tres requisitos que son necesarios para la existencia de este fenómeno: el uso de las TIC, tengan un contenido de carácter sexual y la voluntariedad inicial del titular de esas imágenes.

Sin duda, el uso de las redes sociales ha comportado una nueva forma de interactuar socialmente que ha fomentado que esta práctica sea bastante común. El envío de estas imágenes se percibe como una nueva forma de coqueteo virtual que, lejos de limitarse al ámbito privado, se propaga con el irrefrenable impulso que brindan las TIC, lo que conlleva una serie de consecuencias y riesgos graves para el derecho a la intimidad de sus titulares.

⁹ Cfr. ALCALÉ SÁNCHEZ, M. (2013): “Derecho penal, imagen e intimidad: especial referencia a los procesos de victimización de las mujeres”, *Revista de Derecho Penal y Criminología*, 3.ª Época, núm. 10; p.15. Disponible en: <http://revistas.uned.es/index.php/RDPC/article/view/24555>

Es lógico entonces que sea muy habitual entre jóvenes o menores, como sucede con la difusión de estas imágenes entre los compañeros de clase de la víctima, provocando además de su humillación pública un posible caso de acoso escolar (*Bullying o Cyberbullying*), con graves consecuencias psicológicas para el menor.

En cuanto al carácter sexual de las imágenes, es necesario que la víctima envíe fotos o videos de una conducta sexualmente explícita o, por lo menos, donde se muestre sus órganos sexuales. Quedando fuera de su ámbito las fotografías que simplemente resultan atrevidas o sugerentes sin un contenido sexual expreso, aunque la línea que separa la carga erótica o sexual de un contenido puede resultar a veces difusa¹⁰.

Finalmente, el carácter voluntario inicial de quien envía esas imágenes de contenido sexual a otro constituye un rasgo propio del *Sexting*. En efecto, el tipo exige que “la víctima haya prestado un consentimiento previo para la captación o grabación de imágenes, que se entiende implícito cuando es ella misma la que capta o graba esas imágenes. Sin embargo, para que la conducta sea típica se requiere que a posteriori no medie consentimiento alguno para la difusión, cesión o revelación de esas imágenes a terceros, confiando la víctima en que no iban a salir del círculo íntimo con quien decidió compartirlas”. Está claro que ese previo consentimiento se basa en la relación de confianza que existe entre la persona que consiente en ser grabada o fotografiada en escenas de contenido claramente sexual y la persona destinataria¹¹. De hecho, suele darse en relaciones de pareja o amistad donde las personas tienden a no tomar medidas de precaución porque les resulta imposible imaginar que esas personas las utilicen para hacerles daño. Algo que dista mucho de la realidad como refleja el hecho de que en la mayoría de los casos se cometen por hombres en contra de la expareja cuando han terminado la relación para vengarse. En este último caso, el *Sexting* pasa a convertirse en “Sextorsión”, un chantaje para la víctima que es amenazada con la publicación si no le entrega a cambio dinero, más material de contenido sexual o volver a su anterior relación.

En definitiva, la obtención de estas imágenes no tiene ninguna relevancia penal para

¹⁰ En ese sentido, PÉREZ SAN JOSÉ (2011): *Guía sobre adolescencia y Sexting: qué es y cómo prevenirlo*. cit. p. 7.

¹¹ Cfr. PÉREZ CONCHILLO, E. (2018): *Intimidad y difusión de Sexting no consentido*, Tirant Lo Blanch, Valencia, p.11.

la existencia de este delito, aunque en el momento de la grabación de la imagen el sujeto activo destinatario tenga ya intenciones de revelarla posteriormente. Por tanto, el núcleo característico de su injusto recae en la difusión posterior cuando se quiebra esa relación de confianza que permitió la obtención de la imagen¹².

Atendiendo a lo descrito, el sujeto activo será aquel que lleva acabo la acción típica de difundir, revelar o ceder las imágenes o grabaciones audiovisuales de carácter sexual sin consentimiento de la víctima, a pesar de haberlas obtenido inicialmente con su consentimiento, porque ella se las ha enviado personalmente o ha sido captadas por el propio sujeto activo. Al respecto, la Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado, señala que nos encontramos ante “un delito especial propio del que serían autores aquellos que, habiendo obtenido con la anuencia de la víctima la imagen o grabación comprometida inician, sin autorización del afectado, la cadena de difusión”. Sin necesidad de que se propague a un número considerable de personas, ya que basta para su apreciación, según QUERALT JIMÉNEZ, que “un solo sujeto sea receptor de la acción típica, pues las imágenes ya se encontrarían fuera del ámbito de control de su titular vulnerando su intimidad”¹³.

Respecto al sujeto pasivo, será aquel que vea menoscabada gravemente su intimidad personal por la difusión de estas imágenes o grabaciones audiovisuales de contenido sexual sin su consentimiento. Precisamente, el consentimiento previo para la captación o entrega de imágenes o grabaciones de contenido íntimo era lo que justificaba, antes de la reforma de 2015, que se considerase atípico el *Sexting*, ya que sólo se protegía la difusión, cesión o revelación no consentida de imágenes o grabaciones que hubiesen sido obtenidas sin consentimiento de la víctima. De esta manera, con el art. 197.7 CP se da entrada a supuestos donde la víctima da acceso a una determinada persona a su espacio privado e íntimo y ésta aprovecha tal ocasión para menoscabar gravemente su intimidad compartiendo ese espacio con un tercero. Un aspecto que no presenta ninguna división doctrinal, pues hay unanimidad en la necesidad de este consentimiento previo en la captación y su ausencia en la posterior difusión. Sin embargo, ha sido objeto de crítica que no se especifique sí esa “anuencia

¹² Cfr. CARRASCO ANDRINO, M. (2021): “Descubrimiento y revelación de secretos”. *Tratado de Derecho Penal Español: Parte Especial (I). Delitos contra las personas*. Álvarez García (dir.) y Ventura Püschel (coord.), Tirant lo Blanch, Valencia p. 1466.

¹³ Cfr. QUERALT JIMÉNEZ, J. (2015): *Derecho Penal Español. Parte Especial*. Tirant lo Blanch, Valencia; p.312.

previa” a la que se refiere el precepto deba ser expresa, tácita o ambas.

Otro de los requisitos de este delito es la exigencia de que la divulgación menoscabe gravemente la intimidad de la víctima. Esta exigencia es de gran importancia, ya que aun cuando concurren todas las exigencias típicas anteriores, si no se produce ese menoscabo grave a la intimidad de la víctima no hay delito. De ahí que se considere un delito de resultado que requiere un daño relevante a la intimidad de la víctima, por lo que no cabe cualquier tipo de afectación a la intimidad, sino únicamente las que tengan la consideración de graves. En tal sentido, la Circular 3/2017 de la FGE apunta que se trata de un “elemento que habrá de valorarse caso a caso, en atención a las circunstancias concurrentes a partir del contenido mismo de la grabación, de la situación y condiciones en la que se llevó a efecto, e incluso de las propias características personales de la víctima”.

Por último, el tipo subjetivo exige la concurrencia de dolo, es decir, el sujeto activo tiene que actuar con conciencia y voluntad de divulgar esas imágenes sin consentimiento de su titular. Otra cuestión es su calificación como dolo directo o eventual. Como bien señala la mayoría de la doctrina, en el caso de que “el sujeto activo busque directa e inmediatamente efectuar esta lesión o menoscabo en la intimidad del sujeto pasivo por medio de la difusión del material en cuestión, se podrá apreciar dolo directo.” En cambio, si no se busca directamente ese resultado, pero “se asuma el riesgo de la difusión se podrá estimar dolo eventual porque el resultado no resulta absolutamente improbable”¹⁴. En cualquier caso, no se admite su realización imprudente, por lo que “si la cesión, descubrimiento, o difusión es consecuencia de una conducta negligente, no habrá responsabilidad penal, sin perjuicio de la vía civil”¹⁵.

Sin duda, la pena de prisión de tres meses a un año o multa de seis a doce meses impuesta a este delito ha centrado las críticas de la doctrina tanto por los que se muestran a favor como en contra de su incriminación. Así hay quienes cuestionan su tipificación bien al carácter liviano de la pena porque demuestra “una huida hacia el Derecho penal, cuando la

¹⁴ Cfr. GIL GIL, A./ LACRUZ LÓPEZ, J. M./ MELENDO PARDOS, M./ NÚÑEZ FERNÁNDEZ, J. (2011): *Curso de Derecho Penal: Parte General*, Dykinson, Madrid p. 230.

¹⁵ En tal sentido, DÍAZ TORREJÓN, P. (2017): *Tratamiento penal del Sexting*, Centro de Estudios Jurídicos, Huelva; p. 13. Disponible en: <https://docplayer.es/90950674-Tratamiento-penal-del-sexting-pedro-diaz-torreon-fiscal-de-la-fiscalia-provincial-de-huelva.html>

sanción de esta conducta, si es impropia, correspondería a la jurisdicción civil"¹⁶; bien al principio de intervención mínima que justifica otros mecanismos extrapenales para su castigo como la LO 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. y la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal¹⁷. En cambio, otros defienden su tipificación, pero cuestionan su sanción aludiendo que “la penas no es excesiva en comparación con las establecidas en los demás apartados del artículo 197, si bien le parece desproporcionada en relación con otros delitos de mayor gravedad”¹⁸; o más directamente entienden que esa pena inferior al resto de números del art. 197 “va a causar como efecto un beneficio al autor ciertamente criticable”¹⁹. En este sentido, MENDO ESTRELLA aporta un argumento clave para justificar una mayor penalidad, ya que “la presencia del consentimiento en la grabación de las imágenes por parte de la víctima o la producción por ésta de las mismas puede en muchos casos suponer que las imágenes sean más explícitas y, por ende, más lesiva”²⁰. Mientras que otros defienden la intervención del Derecho penal en este supuesto e incluso que la pena es acertada porque cumple con las exigencias de proporcionalidad²¹.

Probablemente, ese desacuerdo sobre el reproche penal de este tipo de atentados sea la causa de que los tribunales a la hora de imponer la pena valoren tanto la conducta realizada como las repercusiones más o menos graves que se hayan ocasionado a la víctima. Desde mi punto de vista, me parece un factor determinante a la hora de apreciar la magnitud del menoscabo a la intimidad personal de la víctima, ya que cuanto más gente reciba esas imágenes más daño se le habrá ocasionado.

¹⁶ Cfr. QUERAL JIMENEZ (2015): *Derecho Penal Español. cit.*; p. 338.

¹⁷ En ese sentido, BOLEA BARDÓN, C (2015): “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. *Comentarios al Código penal*. Corcoy Bidasolo/Mir Puig (dirs.). Tirant lo Blanch, Valencia, p.732

¹⁸ Cfr. CASTELLÓ NICÁS, N. (2015): “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*. Morillas Cueva (Dir.). Dykinson, Madrid, p. 503.

¹⁹ Cfr. ALCALÉ SÁNCHEZ (2013): *Derecho penal, imagen e intimidad: especial referencia a los procesos de victimización de las mujeres*, cit, p.63.

²⁰ Cfr. MENDO ESTRELLA, A. (2016): “Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al Sexting entre adultos”. *Revista electrónica de Ciencia Penal y Criminología*, núm. 18, Granada p.17. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=5788845>

²¹ En ese sentido, GONZÁLEZ COLLANTES, T. (2015): “Los delitos contra la intimidad tras la reforma de 2015: luces y sombras”. *Revista de Derecho penal y Criminología*, núm. 13, Valencia, p.70. Disponible en: <http://revistas.uned.es/index.php/RDPC/article/view/24520>); y SAINZ-CANTERO CAPARROS, J.E. (2015): “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. *Sistema de Derecho penal: Parte Especial*. 2.ª edición, Morillas Cueva (Dir.). Dykinson, Madrid, p.318.

3.2 Modalidades agravadas

El Código Penal prevé en el inciso segundo del art 197.7 un tipo agravado de *Sexting* en el que se impondrá la pena prevista en su mitad superior (prisión de siete meses y medio a un año o multa de nueve a doce meses) cuando concurren algunas de las siguientes circunstancias:

-Cuando el sujeto activo sea el cónyuge o persona que esté o haya estado unida al sujeto pasivo por análoga relación de afectividad, aún sin convivencia. La introducción de esta agravación se debe a la sugerencia del informe del Consejo General del Poder Judicial al Proyecto de reforma del Código Penal, donde destaca que “se echa de menos que no se haya previsto una agravación cuando la víctima sea el cónyuge o ex cónyuge del sujeto pasivo o persona que conviva o haya convivido con él o mantenga o haya mantenido una relación análoga; excluyendo en este caso la pena de multa por las razones que ya se han expuesto en ese informe”.

En esa misma línea, CARRASCO ANDRINO justifica esta agravación por la cantidad de casos donde la “divulgación viene motivada por el despecho o la venganza, una vez rota la relación amorosa que, en muchas ocasiones, se presenta como una forma de violencia de género. Si bien el fundamento de la agravación no reside en la violencia de género”. Si bien, aclara que el fundamento de la agravación no reside en la violencia de género, pues “no se limitan los sujetos activo o pasivo por razón del género, sino por la estrecha relación de afectividad que implica la relación matrimonial o la análoga a esta, y que implican actividades de intimidad compartida, cerradas al conocimiento de terceros distintos de la pareja”²².

-Cuando el sujeto pasivo sea menor de edad o persona con discapacidad que necesita de especial protección. Su previsión responde a la voluntad del legislador de otorgar una mayor y más efectiva protección a los sujetos que requieren de especial protección y tutela.

Respecto a la persona discapacitada necesitada de especial protección no plantea problemas porque se atiende a lo establecido en el art 25 CP:

²² Cfr. CARRASCO ANDRINO (2021): “Descubrimiento y revelación de secretos”. *cit.*; p.1470.

“A los efectos de este Código se entiende por discapacidad aquella situación en que se encuentra una persona con deficiencias físicas, mentales, intelectuales o sensoriales de carácter permanente que, al interactuar con diversas barreras, puedan limitar o impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás. Asimismo, se entenderá por persona con discapacidad necesitada de especial protección a aquella persona con discapacidad que, tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus deficiencias intelectuales o mentales de carácter permanente”.

Mientras que la minoría de edad sugiere la cuestión de si estas víctimas tienen capacidad para que su consentimiento previo a la divulgación sea válido. Un sector doctrinal considera que los catorce años es la edad mínima para que el consentimiento del menor tenga relevancia, aunque debe exigirse en todo caso un análisis de su capacidad de juicio. De manera que solo se consideraría válido penalmente su consentimiento si se apreciara un grado de madurez suficiente. Su fundamento reside en la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales, que dispone que “el tratamiento de los datos personales de un menor de edad únicamente podrá basarse en su consentimiento cuando sea mayor de catorce años” (art.7). Otra parte de la doctrina que entiendo más razonable defiende que el consentimiento válido de un menor ha de ser a los dieciséis años, acorde con la elevación de la edad penal para consentir en materia sexual efectuada por la reforma penal de 2015, en respuesta a la Directiva 2011/93/UE, que establece que todo acto sexual con un menor de esa edad es abusivo y delictivo.

En todo caso, debe tenerse en consideración que las imágenes y vídeos de contenido sexual cuyos protagonistas son menores de edad o discapacitados puede constituir un delito de pornografía infantil del art. 189 CP, siendo entonces irrelevante el consentimiento del menor. Asimismo, el mero intento de convencer al menor de dieciséis años para que participe en una conducta de *Sexting* puede ser constitutivo de un delito de embaucamiento del art 183.2 ter CP, también conocido como *Child Grooming*. En este precepto se tipifica como delito “el que a través de internet, del teléfono o de cualquier otra tecnología de la

información contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años”.

- Por último, cuando los hechos se cometan con el objetivo de obtener un lucro. Esto es, el ánimo de lucro propio de los delitos patrimoniales, entendido como “finalidad de enriquecimiento económico propio o ajeno”²³. La mayoría de la doctrina explica esta motivación en la necesidad de evitar el posible comercio ilícito de datos tan sensibles relativos a la intimidad de sus afectados.

Una finalidad que no podrá ser sobrevenida, ya que debe darse de manera simultánea o anterior al momento en que se lleva a cabo la difusión multimedia de esas imágenes o videos. No obstante, su apreciación resulta problemática puesto que la voluntad de querer lucrarse pertenece al ámbito subjetivo del autor, por lo que habrá que acudir a indicios objetivos que permitan comprobar esta circunstancia para la apreciación de la agravante. Un ejemplo donde podría apreciarse sería el caso de quien hubiera pactado un precio con un tercero a cambio de recibir esas imágenes íntimas a través de redes sociales como *WhatsApp* o páginas web de contenido sexual.

IV. NUEVAS INICIATIVAS DE PROTECCIÓN PARA LAS VÍCTIMAS DE CIBERDELITOS: EL DERECHO AL OLVIDO DIGITAL

En una sociedad marcada por las TIC y la expansión globalizada de Internet resulta usual la transmisión inmediata de información a una gran velocidad y el almacenamiento de datos personales de los ciudadanos. Cuando una persona acaba siendo víctima de *Sexting* pierde el control total sobre sus imágenes más íntimas ya que lo que se cuelga en la red queda almacenado para siempre y cualquiera puede tener acceso a él con facilidad, sin necesidad de ser un experto que tengan unos grandes conocimientos técnicos sobre Internet.

²³ Cfr. HERAS VIVES, L. (2017): *La protección penal de la intimidad: una revisión crítica a propósito del nuevo artículo 197.7 del Código Penal Español*, Tesis doctoral de la Universidad Autónoma de Barcelona, p. 639. Disponible en: <https://ddd.uab.cat/record/189646?ln=ca>

En efecto, Internet registra grandes cantidades de información -fotos en línea, participaciones en foros, acciones vergonzosas publicadas en las redes sociales, etc.-, que no desaparecen ni se olvida nunca. Es más, los motores de búsqueda como *Google*, *Yahoo!*, entre otros, ayudan con la simple introducción del nombre y los apellidos de un individuo a encontrar otros datos más íntimos que su identidad. Esa accesibilidad ilimitada a cualquier información o contenido sobre una persona puede llegar a causarles un perjuicio añadido a la ya grave invasión de su intimidad. Así lo reflejan las encuestas realizadas por el V Informe sobre Redes Sociales y Mercado de Trabajo de 2016, que aseguran que “el 86% de las empresas utilizan redes sociales como *Facebook* para ver el perfil de la persona a la que van a contratar”. El conocimiento de determinados datos de manera aislada, según este informe, “puede generar reacciones desfavorables por parte de terceros creando una incidencia negativa en nuestra carrera profesional, académica o incluso en nuestras relaciones sociales. Estar atados al pasado o que se nos juzgue nuestro valor actual a partir de acciones pasadas constituye un menoscabo del respeto que merecemos”²⁴.

Ante este tipo de situaciones, la necesaria intervención del Derecho penal no resulta suficiente, es necesario además proporcionar a los afectados una serie de medidas para proteger de forma efectiva su intimidad y poner freno a la capacidad de recordar toda la vida digital de las personas. Si tenemos libertad, también debemos tener derecho al olvido.

4.1 ¿Qué es el olvido digital?

Existe una verdadera preocupación sobre el futuro de la generación más joven que está dejando su trayectoria de vida grabada en la red cuando se vea perseguida por el recuerdo de su pasado. Una de las respuestas que ofrece el derecho para los usuarios de las redes sociales e Internet es intentar suprimir aquella información personal que pueda afectar su privacidad, lo que se conoce como el derecho al olvido.

Nos referimos a un derecho que, según SIMÓN CASTELLANO, posibilita que “los datos de las personas físicas dejen de ser accesibles en la web por petición de ellas y cuando estas lo decidan”; por lo que se puede entender como “el derecho a retirarse del sistema y

²⁴ Disponible en: <https://cdn.infoempleo.com/infoempleo/documentacion/publicaciones/Informe-Infoempleo-Adecco-sobre-Mercado-de-Trabajo-y-Redes-sociales-2017.pdf>

eliminar la información personal que la red contiene”²⁵.

Pareciera que asistimos a una actualización de los clásicos derechos de cancelación y oposición al mundo digital, aunque aplicados exclusivamente a los buscadores y redes sociales. Sin embargo, los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), que permiten a una persona física ejercer un control sobre sus datos personales, cuando se aplican a las redes sociales no constituyen una solución real del problema, ya que durante todo el tiempo que esa información es pública queda expuesta y es susceptible de ser copiada o descargada por diferentes usuarios a nivel global. Por tanto, no parece posible lograr la eliminación total y efectiva de la información, aunque se pueda llegar a garantizar el control de su difusión y acceso.

El fundamento del derecho al olvido descansa en dos derechos fundamentales: el derecho a la intimidad, consagrado en el art. 18.1 CE como un derecho personalísimo que faculta a su titular a impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, independientemente del fin perseguido; y el derecho a la protección de datos que, a pesar de no tener una mención directa en nuestra Constitución, el legislador actualizó el art. 18.4 a la nueva realidad social al reconocer los riesgos del uso de la informática y establecer limitaciones en su uso. Se entiende así que se trate, como señala DÍEZ-PICAZO GIMÉNEZ, de un derecho de configuración legal que “implica un desdoblamiento de las normas de referencia que, en este caso al no regir el respeto a la configuración constitucional del derecho fundamental como criterio de referencia, éste vendrá dado por la unión entre la norma constitucional y las normas de desarrollo”²⁶. Por lo que a la hora de definir la naturaleza jurídica de este derecho se puede clasificar como “un derecho humano, fundamental, subjetivo y de la personalidad”²⁷.

El titular de este derecho sería toda persona física. La mayoría de la doctrina excluye de su titularidad a las personas jurídicas, ya que los derechos fundamentales no pueden ser atribuidos a las mismas. En contra, un sector minoritario considera que esa concepción

²⁵ Cfr. SIMÓN CASTELLANO, P. (2012): *El Régimen Constitucional del Derecho al Olvido Digital*, Tirant Lo Blanch, Valencia, p.21.

²⁶ Cfr. DÍEZ-PICAZO GIMÉNEZ, L. (2013): *Sistema de Derechos Fundamentales*. Civitas, Madrid, p. 120.

²⁷ Cfr. ARENAS RAMIRO, M. (2015): “Reforzando el ejercicio del derecho a la protección de datos” en *Hacia un nuevo Derecho europeo de Protección de Datos*. Rallo Lombarte/García Mahamut (Coords.), Tirant lo Blanch, Valencia, p. 335.

clásica ha de evolucionar, en tanto que sí no todos los derechos fundamentales pueden ser extrapolables a las entidades, existen algunos como el derecho al honor que le han sido reconocidos por la jurisprudencia y no se puede negar la fuerte conexión entre ambos derechos. Sostienen también que resulta difícil negar que no se le pueda causar un perjuicio a la reputación de una sociedad por el tratamiento de datos falsos o pasados, obstaculizando su funcionamiento y desarrollo económico, dejando a las entidades desprotegidas sin poder ejercer ninguna acción penal contra ese daño.

El usuario deberá primero solicitar a la persona responsable de subir el contenido a la red su eliminación, y en caso de negarse pedirá a la red social o la plataforma donde se encuentran publicadas esas imágenes o vídeos su eliminación mediante la identificación de los enlaces en los que se contienen los datos que se pretenden eliminar. Las redes sociales más conocidas como *Twitter*, *Instagram* y *Facebook* o uno de los motores de búsqueda más famoso como *Google*, en un intento de hacer más sencillo a sus usuarios reclamar ante este tipo de delitos han añadido una pestaña que pone “Denunciar” al lado de cada contenido multimedia que se encuentra en sus plataformas. Después de interponer la reclamación, la empresa tiene la obligación de resolver la solicitud en el plazo máximo de un mes a contar desde la recepción de esta.

Es cierto que este derecho al olvido tiene un cierto recorrido histórico, pero aún es de carácter novedoso, por lo que todavía nos encontramos ante un concepto jurídico que no está “pacíficamente delimitado”²⁸. Más bien, podría decirse que es un concepto en evolución, que conforme se va integrando en las distintas normas nacionales e internacionales y en las resoluciones de los órganos jurisdiccionales, se perfila mejor su objeto y definición.

Desde su consolidación en España ha existido un incremento de las demandas interpuestas por este derecho, hasta el punto de que en cinco años los españoles han rellenado casi 80.000 reclamaciones para pedir eliminar este tipo de datos en los buscadores²⁹. Con todo, cuando estas peticiones son resueltas con una negativa de las entidades o simplemente dan una respuesta insatisfactoria, hay otras opciones para ejercer este derecho como la

²⁸ Vid. RALLO LLOMBARTE, A. (2014): *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, p.17

²⁹ Datos del blog *Legal Today*, disponible en: <https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/los-ciudadanos-espanoles-remiten-casi-80000-peticiones-para-ejercer-su-derecho-al-olvido-en-internet-ante-google-en-cinco-anos-2019-06-03/>

Agencia Española de Protección de Datos (AEPD), que con su actividad diaria ha desempeñado un papel esencial en el reconocimiento del derecho al olvido digital en nuestro país.

En efecto, La AEPD configura este derecho, por un lado, para ejercitar el derecho de cancelación de los datos que la red conserva cuando exista una finalidad legítima (cultural o histórica, por ejemplo) que proteja la publicación; y por otro, exigir que el buscador encuentre medios para que la información no vuelva a aparecer en el futuro. Para ello, ha desarrollado una serie de instrumentos como el denominado “Canal Prioritario” para la atención prioritaria de casos de difusión de imágenes o videos sexuales cuyo objetivo es evitar con la mayor rapidez posible su difusión masiva. Esta herramienta está a disposición de la propia persona afectada por la publicación del contenido multimedia o de un tercero que haya podido recibir ese contenido y quiera denunciar estos hechos para no ser cómplice de la difusión. Una vez analizada la reclamación por la AEPD ordenará a la plataforma donde se encuentre esas imágenes o vídeos publicados su retirada, al tiempo de que si existen indicios de delito se pondrá en contacto con la Fiscalía para que tramite el correspondiente procedimiento penal contra las responsables de la difusión.

Si bien, su labor va mucho más allá. Hay que destacar su importante papel de concienciación mediante campañas de información dirigidas principalmente a adolescentes. En 2020 consiguieron hacer viral la campaña “Puedes Pararlo”, en la que participó una poeta e *influencer* llamada Elvira Sastre, donde relataba en *Twitter* que estaba siendo víctima de *Sextorsión* por una antigua pareja que tenía un video comprometido suyo que accedió a grabar cuando mantenían esa relación. A pesar de que no era cierta la historia, al contarla de una manera tan personal y cercana logró captar la atención de sus jóvenes seguidores a los que, además de dar a conocer el Canal Prioritario por si lo necesitaban en un futuro, logró crear una mayor sensibilización sobre los peligros que comporta el *Sexting*.

Tal herramienta resulta muy eficaz cuando se trata de redes sociales, ya que se perciben hoy en día como un contexto despreocupado donde la publicación de contenidos se hace entre amigos sin correr peligros. Por ello, hay que concienciar tanto a los partícipes de este tipo de prácticas sexuales *online* para que tomen las precauciones necesarias como a los terceros que reciban estas imágenes para que no contribuyan a su difusión. Un ejemplo que muestra como la concienciación puede lograr grandes cambios en la lucha de la difusión de contenidos sin consentimiento, se ha podido ver a finales de 2020. Me refiero al artículo en

el *The New York Times* del periodista Nicholas Kristof., quien destapó como una famosa web que distribuía contenido pornográfico se encontraban millones de videos publicados por venganza, grabaciones no consentidas y abusos sexuales de menores, entre otros, lo que obligó a *MasterCard* y *Visa* a bloquear los pagos con sus tarjetas de esta web³⁰. Tras recibir esta noticia en menos de 24 horas la web pasó de tener 13 millones de videos a rozar los 3 millones, lo que llevó a cambiar la política de su web permitiendo subir contenido solo a usuarios cuya identidad y edad esté legalmente acreditada y obligando a los empleados a revisar cada uno de los videos antes de estar disponibles³¹.

Sin duda, esta serie de medidas muestran el camino que debe extenderse por todo el mundo digital, porque suponen un gran avance no solo en la seguridad de los usuarios, sino también en la protección de las víctimas de ciberdelitos.

4.2 La consagración del derecho al olvido en la Unión Europea: especial referencia al caso español

Cada vez más el papel de los jueces no se limita a la simple interpretación de las leyes, ya que como bien apunta ÁLVAREZ GARCÍA, su función “ha trascendido la mera subsunción y ha asumido, cada vez más tareas creadoras, sin descuidar, en ningún caso, su obligación de sumisión a la ley, al principio de legalidad y de seguridad jurídica”³².

Es precisamente lo que ha sucedido en esta materia, donde el precursor indiscutible del derecho al olvido digital ha sido el Tribunal de Justicia de la Unión Europea (en adelante, TJUE), en el asunto *Google-Costeja* de la Sentencia 13 de mayo de 2014 (C-131/12). Se trata del primer pronunciamiento judicial sobre la cuestión que va a sentar las bases para su aplicación y denominación a esta nueva garantía jurídica para la protección de datos personales. Este litigio entre *Google* frente a un ciudadano español y la AEDP surge cuando esta última resuelve favorablemente una reclamación contra este motor de búsqueda y la empresa La Vanguardia S. L. Se refería a una noticia que transcurridos más de quince años

³⁰ Cfr. DONABET KRISTOF, N. (2020): “The Children of Pornhub” en *The New York Times*. Disponible en: <https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html>

³¹ Datos del Diario La Vanguardia, Disponible en: <https://www.lavanguardia.com/vida/20201214/6121227/pornhub-elimina-mas-mitad-videos-revisar-contenido-ilegal.html>

³² Cfr. ÁLVAREZ GARCÍA, F. (2009): *Sobre el principio de legalidad*. Tirant lo Blanch, Valencia, p. 175.

desde su publicación aún era accesible, donde se relataba que el demandante había sido condenado por una serie de impagos, perjudicando con ello su imagen social y profesional actual. Se entendía que constituía una información desfasada, ya que ese embargo ya había sido resuelto y el afectado no presentaba ya relación alguna con deudas ni empresas embargadas. Ante la complejidad del caso, se consideró oportuno interponer una cuestión prejudicial al TJUE, quien en su pronunciamiento estableció que el tratamiento de datos personales por parte de los buscadores podía afectar a los derechos de respeto a la vida familiar y a la protección de los datos personales, sobre todo cuando esa búsqueda se hacía a partir del nombre de una persona física, pues permitía a cualquier usuario juzgar una persona en base a la lista de resultados ofrecida.

El punto más novedoso de esta resolución es que alude a datos o informaciones verídicas o lícitas, que si se conservan por un tiempo superior al necesario puede considerarse inadecuado su uso. Tal consideración obligó al motor de búsqueda a eliminar los resultados de tal información porque el tratamiento de datos debe ser legítimo durante todo el periodo en que se lleve a cabo. Esta sentencia supuso todo un cambio y evolución del Derecho, ya que otorga a los internautas más seguridad sobre cómo deben ser tratados sus datos por parte de los motores de búsqueda. Como afirma ARENAS RAMIRO, esta sentencia y otras sucesivas resoluciones sobre el derecho al olvido ha convertido al TJUE “en un auténtico juez garante de la privacidad ante la evolución tecnológica global”³³.

Está claro que las instituciones europeas han entendido que ante el amplio alcance que se puede dar al tratamiento de datos en una sociedad globalizada, ya no son suficientes las leyes internas de un estado para proteger la privacidad de los usuarios. Por ello, se ha llevado a cabo un proceso de unificación y actualización de las normas jurídicas de todos los países de la Unión Europea (en adelante, UE) para que se sometan a una misma regulación en esta materia, dando lugar al nuevo Reglamento General Europeo de Protección de Datos (2016/679), de 27 de abril de 2016. En este texto se recoge expresamente en su art. 17 la regulación del derecho al olvido bajo la denominación “derecho de supresión”, que reconoce que el interesado tiene derecho a que el responsable del tratamiento y divulgación de los datos sea quien los suprima y se abstenga de darles más difusión cuando se dé alguna de estas circunstancias siguientes:

³³ Cfr. ARENAS RAMIRO, M. (2006): “El derecho a la protección de datos personales en la jurisprudencia del TJCE”. *Revista de Derecho y Nuevas Tecnologías*, Vol. 4, Aranzadi Thomson Reuters, p.97.

-los datos personales ya no son necesarios acorde con los fines para los que fueron recogidos o tratados.

-el interesado retire el consentimiento que había dado anteriormente.

-el interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para mantenerlos.

-los datos personales hayan sido tratados ilícitamente

-los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento

-los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información

Al tiempo que reconoce que este derecho no es absoluto, por lo que establece una serie de circunstancias en las que no es posible aplicar el derecho al olvido porque el tratamiento de esos datos sea necesario para algunos de los fines siguientes:

-ejercer el derecho a la libertad de expresión e información.

-cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable

-razones de interés público en el ámbito de la salud pública.

-fines de archivo en interés público, de investigación científica, histórica o estadísticos, en la medida en que el derecho al olvido pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.

-formulación, ejercicio o defensa de reclamaciones.

Esta nueva regulación otorga por primera vez al interesado la potestad de gestionar su información personal según sus preferencias, pasando las empresas y administraciones a un segundo plano con la obligación de cambiar sus políticas de protección de datos. Si bien, no es la única novedad que aporta este Reglamento, ya que también pone fin al problema de territorialidad al extender su regulación a responsables del tratamiento de datos que, sin estar

establecidos en la Unión Europea, sus actividades estén relacionadas con ciudadanos residentes, pudiendo actuar los poderes legislativo y judicial sin ningún impedimento como antes ocurría. De este modo, como bien reconoce SANCHO LÓPEZ, se pone fin a “la práctica consolidada entre las corporaciones de Internet de establecer sus sedes en países cuyas legislaciones permiten sin demasiados problemas la mercantilización de la información personal, ignorando reiteradamente la legislación doméstica y europea en la materia e impidiendo el ejercicio eficaz de los derechos de los ciudadanos a quienes dejaba en una situación jurídica de indefensión”³⁴.

Cabe preguntarse, entonces, qué pasa si aun ejerciendo el derecho al olvido los responsables de este tratamiento de datos no cumplen con su obligación. Pues bien, el Reglamento prevé esta posibilidad en su art. 83.5 apartado b), que estipula que en estos casos “se sancionará mediante multas administrativas de 20.000.000 € como máximo o en el caso de que se trate de una empresa de una cuantía equivalente al 4 % un máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”.

Sin embargo, tampoco está exento de críticas. Una parte de la doctrina opina que el Reglamento está lleno de términos jurídicos indeterminados que recae su interpretación sobre los órganos jurisdiccionales, lesionando así la separación de poderes. O que realiza demasiadas remisiones para que los Estados miembros sean quienes regulen aspectos jurídicos, lo que parece contrario a esa armonización que lo inspiró y al fin que se pretendía con esta normativa, evitar discrepancias entre las legislaciones de los diferentes estados.

En el caso de España, el Reglamento era el único instrumento normativo que regulaba de forma vinculante el derecho al olvido hasta la aprobación de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, donde se contempla este derecho bajo la denominación “derecho de supresión” (art. 15) y “derecho al olvido” (arts. 93 y 94).

Con este texto legal, legislador mantiene gran parte de esta normativa europea, desarrollando su contenido a supuestos concretos sucedidos en nuestro país. Así se refleja en su similitud en la regulación del derecho al olvido en búsquedas de Internet, donde su

³⁴ Cfr. SANCHO LÓPEZ, M. (2020): *Derecho al olvido y big data: dos realidades convergentes*, Tirant Lo Blanch, Valencia, p. 74

redacción está muy influenciada por el caso *Google* y demás jurisprudencia del TJUE en casos parecidos, cuando reconoce el derecho que ostentan las personas a “solicitar a los motores de búsqueda de internet que eliminen las listas de resultados que se efectúen como consecuencia de introducir los nombres y apellidos cuando estos datos sean, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información” (art. 93). O al regular el derecho al olvido en las redes sociales y servicios equivalentes, donde permite ejecutarlo a solicitud del interesado frente a estas organizaciones, con la supresión de la información facilitada por el afectado o por una tercera persona cuando estos datos sean dañinos (art. 94).

En cambio, añade como novedad el derecho de supresión en aquellos datos que hayan sido facilitados cuando el afectado sea menor de edad, aunque no concurren las circunstancias previstas en los casos anteriormente mencionados: “En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurren las circunstancias mencionadas en el apartado 2” (art 94.3). Su introducción ha sido alabada por la mayoría de la doctrina, ya que considera que el ejercicio del derecho al olvido no debería limitarse a los motores de búsqueda para ofrecer una protección más amplia en el tratamiento de datos, junto a la necesidad de mayor protección a los menores de edad en un abanico más amplio de situaciones que hasta entonces se venían dando.

V. APLICACIÓN JUDICIAL DEL OLVIDO DIGITAL EN NUESTRO PAÍS

Los tribunales han sido una de las partes más importantes en la configuración de este derecho en nuestro sistema jurídico, ya que mediante sus resoluciones han establecido su forma de aplicación y sus límites. Hasta el punto de que, tras la sentencia del TJUE en el caso *Google-Costeja*, el incremento de reclamaciones interpuestas por los internautas ha provocado numerosos pronunciamientos sobre el tema.

El primer pronunciamiento fue la Sentencia de la Audiencia Provincial de Barcelona 486/2013, de 11 de octubre, donde se estimó la demanda interpuesta por dos ciudadanas contra Ediciones El País S.L, ya que cuando se insertaban sus nombres en los motores de

búsqueda aparecía una noticia de 1985 debido a la digitalización de la hemeroteca del periódico. La noticia exponía a las afectadas porque, además de mencionarlas con nombre y apellido, aludía a que el síndrome de abstinencia le había llevado a realizar un delito de tráfico de drogas por el que fueron condenadas. En esta demanda se alegó una vulneración de sus derechos de protección de datos, intimidad y honor, que no estaba amparada por la libertad de expresión porque las demandantes habían superado su adicción y sus antecedentes penales se encontraban cancelados por ese asunto. Con todo, lo más relevante de esta resolución es que vinculó el derecho al olvido con el derecho a la intimidad, dándole a este último un sentido mucho más amplio del que se venía dando, al entender que la publicación de tales datos personales que las hacía plenamente identificables eran innecesarios para la difusión de la noticia en cuestión. En ese sentido, argumenta el tribunal que se debe partir del derecho al olvido como derecho a la privacidad y parte de los derechos de la personalidad. “Una vez pagado lo debido, la sociedad debe ofrecerle la posibilidad de rehabilitarse e iniciar una nueva vida sin tener que soportar el peso de sus errores del pasado el resto de su vida”. Por tanto, lo que se pretende impedir es que salga en una noticia que pueda perjudicar a una persona que nunca tuvo carácter de figura pública o de relevancia social en la historia de nuestro país.

Esta sentencia es considerada una de las más importantes porque establece lo que serán los cimientos de una jurisprudencia consolidada en materia del derecho al olvido a pesar de que más tarde fuese recurrida, primero ante el Tribunal Supremo donde se estimó parcialmente el recurso presentado y después ante el Tribunal Constitucional. En efecto, la Sentencia del Tribunal Supremo de la Sala de lo Civil 454/2015 de 15 de octubre, que resuelve el recurso presentado por Ediciones El País S.L, reafirma la vinculación existente entre los datos personales y el derecho al honor y a la intimidad, afirmando así la existencia de un derecho al olvido. La novedad es que plantea una ponderación entre la libertad informativa y el derecho al olvido, dando una gran importancia al factor del tiempo. En ese sentido, afirma que “El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los principios de calidad de datos no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento”. Un tratamiento que sí inicialmente pudo ser adecuado a la finalidad que lo justificaba “puede devenir con el transcurso del tiempo inadecuado para esa finalidad, y el daño que cause en derechos de la personalidad como el honor y la intimidad, desproporcionado en relación con el derecho que ampara el tratamiento

de datos”.

Esta resolución tiene un interés vital, no solo por el reconocimiento del derecho al olvido, sino por el escaso límite que impone a la inalterabilidad de las hemerotecas. Con todo, considera que “la integridad de los archivos digitales debe gozar de la protección del derecho a la libertad de información, ya que satisface un interés público ese acceso a la información, sin que se altere o borre su contenido, ni siquiera dando la posibilidad de que se sustituyan los nombres por iniciales”. De este modo, deja sin valor las medidas de supresión de datos personales impuesta por la anterior instancia, que la califica de sacrificio desproporcionado de la libertad de información protegida en el art. 20.1.d CE.

Tras presentar las afectadas un recurso de amparo ante el Tribunal Constitucional, se produce el primer pronunciamiento del Alto Tribunal sobre la materia en la STC 58/2018, de 4 de junio, que impone algunos nuevos límites. Entiende que las hemerotecas digitales deberían eliminar la opción de búsqueda por nombres y apellidos en sus buscadores internos de la web, ya que “se trata de una medida limitativa de la libertad de la información idónea, necesaria y proporcionada al fin de evitar una difusión de la noticia lesiva de los derechos invocados. La medida requerida es necesaria porque su adopción y solo ella, limitará la búsqueda y localización de la noticia en la hemeroteca digital sobre la base de datos personales inequívocamente identificativos”. De esta manera, a pesar de que no modifica el límite que no se considera ajustado a derecho, la eliminación de los nombres publicados en las noticias en papel consigue dar una protección acorde al derecho al olvido al desaparecer estos resultados en las búsquedas. Si bien, el tribunal hace mención también que “el importante papel que tiene la información pública en una sociedad democrática no debe de tener más importancia que el derecho a la privacidad”, ya que una noticia de hace 30 años que se le siga dando publicidad posibilita unos daños desproporcionados a los implicados.

En definitiva, lo más relevante de esta sentencia es que se atribuye un carácter fundamental y autónomo al derecho al olvido respecto del derecho a la protección de datos personales, la intimidad y el honor, ya que “al reconocerlo como derecho fundamental, supone su automática aplicación por la jurisprudencia relativa a los límites de los derechos fundamentales”.

Un año después, la STS de la Sala Contencioso-Administrativa 12/2019, de 11 de enero, decidió desestimar un recurso de casación presentado por *GOOGLE INC* en contra de la Sentencia de la Audiencia Nacional 3029/2017 de 18 de julio, que reconocía el derecho al olvido al afectado que, al introducir su nombre y apellidos, aparecía una noticia publicada en un periódico que describía una serie de hechos que eran parcialmente inexactos. Según el tribunal “la persona afectada por una supuesta lesión del derecho al honor, a la intimidad personal y familiar y a la propia imagen está legitimada para fundamentar válidamente una acción de reclamación ante la entidad proveedora de los servicios de motor de búsqueda que ofrezcan datos sustancialmente erróneos o inexactos que supongan una desvalorización de la imagen reputacional que se revele injustificada por contradecir los pronunciamientos formulados en una resolución judicial firme”. De este modo, esta resolución establece una doctrina que garantiza la protección de aquellas personas que mediante los motores de búsqueda web difundan noticias con datos inexactos.

En 2020, la Sala de lo Contencioso-Administrativo del Tribunal Supremo volvió a pronunciarse sobre el derecho al olvido en la Sentencia 1624/2020, del 27 de noviembre. En ella se analizaba a un usuario que solicitó a la compañía *Microsoft Corporation*, propietaria del buscador web *Bing*, que desvinculase una serie de *urls* para aquellas búsquedas que se realizasen no solo con su nombre y apellidos, sino también cuando se introdujesen sus dos apellidos. La compañía solo consideró adecuado la primera petición, al igual que más tarde la AEPD y la Audiencia Nacional en la Sentencia 3093/2019, del 22 de julio de 2019 se mostraron a favor de la compañía, al considerar que el Registro Civil identificaba a las personas por su nombre completo y no por los apellidos. Frente a esta postura, esta sentencia consideró que se debía aceptar ambas peticiones, ya que “la supresión de datos resultaba coherente con la jurisprudencia europea que, además de reconocer el derecho a la eliminación de búsquedas a partir de un nombre, sin distinguir si se refiere al nombre, a los apellidos o a ambos juntos; también reconoce el derecho al olvido como derecho fundamental en el marco garantista de las libertades informáticas”. En resumen, entiende que no debe interpretarse de forma tan restrictiva una referencia al tratamiento de datos de carácter personal en base a la normativa interna del Registro Civil, ya que esto “supondría ir en contra de la finalidad tuitiva de la normativa tanto europea como nacional de protección de datos de carácter personal”.

Esta sucesión de criterios respecto al derecho al olvido por parte de la jurisprudencia nos muestra que los límites sobre el derecho de información están en constante evolución para perfilar una aplicación más precisa de este derecho en nuestro país.

VI. CONCLUSIONES

El siglo XXI es sin duda el de las TICS. Internet y los avances tecnológicos han impactado de tal manera en la sociedad que se han visto afectados cada uno de los aspectos de nuestra vida. Hasta tal punto que se ha creado incluso dos tipos de sociedades. Por un lado, la sociedad a nivel físico donde los bienes jurídicos se dañan de una manera material y perceptible. Y por otro, la sociedad virtual donde también se vulneran los mismos bienes jurídicos de forma igual o incluso más lesiva, obligando a actualizar la incriminación de los delitos tradicionales.

Está claro que el uso de las TICS constituye un arma de doble filo ya que, junto a las grandes mejoras y avances que comportan, también facilitan nuevas modalidades de delinquir como el *Sexting*. Esta nueva cibercriminalidad ha obligado a revisar la tipicidad de ciertos delitos ante la grave repercusión que estos nuevos atentados suponen para derechos tan relevantes como la intimidad. Así sucedió en nuestro país con el caso de Olvido Hormigos que dio pie a la reforma de 2015 de nuestro texto punitivo.

Surgen así la necesidad de adoptar nuevas formas de protección a las víctimas de ataques informáticos, junto a campañas de concienciación en la red o el canal prioritario de la AEDP, entre otros. Una de las medidas más importantes es la regulación del derecho al olvido como derecho fundamental que permite cancelar y borrar aquellos datos personales a los que cualquiera puede tener acceso, siempre que no se trate de una información de interés público, para evitar ese grave peligro a nuestra intimidad, honor e integridad moral.

Así se reconoció en primer lugar por la jurisprudencia internacional en el caso *Google-Costeja*, y posteriormente por nuestras instancias judiciales que se han encargado de perfilar la aplicación y los límites de este derecho. Una jurisprudencia que sigue en constante evolución adaptándose a los continuos avances y desafíos que presenta la sociedad tecnológica de nuestros días para ofrecer una respuesta penal adecuada a estas nuevas formas de criminalidad virtual.

VII. BIBLIOGRAFÍA

AGUSTINA, J. R./GÓMEZ-DURÁN, E. L. (2016): “Factores de riesgo asociados al Sexting como umbral de diversas formas de victimización. Estudio de factores correlacionados con el Sexting en una muestra universitaria”. *Revista de Internet, Derecho y Política*, núm. 22.

ALCALE SÁNCHEZ, M. (2013): “Derecho penal, imagen e intimidad: especial referencia a los procesos de victimización de las mujeres”. *Revista de Derecho Penal y Criminología*, 3.ª Época, núm. 10.

ÁLVAREZ GARCÍA, F. (2009): *Sobre el principio de legalidad*. Tirant lo Blanch, Valencia.

ANGUITA OSUNA, J.E. (2018): “Análisis histórico-jurídico de la lucha contra la ciberdelincuencia en la Unión Europea”. *Revista de Estudios de Seguridad Internacional*. Vol. 4, núm. 1.

ARENAS RAMIRO, M. (2006): “El derecho a la protección de datos personales en la jurisprudencia del TJCE”. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Vol. 4, Aranzadi Thomson Reuters.

ARENAS RAMIRO, M. (2015): “Reforzando el ejercicio del derecho a la protección de datos” en *Hacia un nuevo Derecho europeo de Protección de Datos*. Rallo Lombarte/García Mahamut (Coords.), Tirant lo Blanch, Valencia.

BOLEA BARDÓN, C. (2015): “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. *Comentarios al Código penal*. Corcoy Bidasolo/Mir Puig (dirs.), Tirant lo Blanch, Valencia.

CARRASCO ANDRINO, M. (2021): “Descubrimiento y revelación de secretos”. *Tratado de Derecho Penal español: Parte Especial (I). Delitos contra las personas*, Álvarez García (dir.) y Ventura Püschel (coord.), Tirant lo Blanch, Valencia.

CASTELLÓ NICÁS, N (2015) “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio” *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)* Morillas Cuevas (Dir.). Dykinson, Madrid.

DAVARA RODRIGUEZ, M. (1993): *Derecho informático*. Editorial Aranzadi, Madrid.

DÍAZ TORREJÓN, P. (2017): *Tratamiento penal del Sexting*, Centro de Estudios Jurídicos, Huelva.

DÍEZ-PICAZO GIMÉNEZ, L. (2013): *Sistema de Derechos Fundamentales*, Civitas, Madrid.

GIL GIL, A./ LACRUZ LÓPEZ, J. M./ MELENDO PARDOS, M./ NÚÑEZ FERNÁNDEZ, J. (2011) *Curso de Derecho Penal. Parte General*, Dykinson, Madrid.

GONZÁLEZ COLLANTES, T (2015): “Los delitos contra la intimidad tras la reforma de 2015: luces y sombras”. *Revista de Derecho penal y Criminología*, núm. 13, Valencia.

HERAS VIVES, L. (2017): *La protección penal de la intimidad: una revisión crítica a propósito del nuevo artículo 197.7 del Código Penal Español*. Tesis doctoral de la Universidad Autónoma de Barcelona.

MARTÍNEZ ATIENZA, G. /BERMEJO FERNANDEZ. D. (2020): *Ciberdelitos*, Ediciones Experiencia.

MENDO ESTRELLA, A (2016) “Delitos de descubrimiento y revelación de secretos: acerca de su aplicación al Sexting entre adultos”. *Revista electrónica de Ciencia Penal y Criminología*, número 18, Granada.

PÉREZ CONCHILLO, E. (2018): *Intimidad y difusión de Sexting no consentido*. Tirant Lo Blanch, Valencia.

QUERALT JIMÉNEZ, J. (2015): *Derecho Penal Español. Parte Especial*. Tirant lo Blanch, Valencia.

RALLO LLOMBARTE, A. (2014): *El derecho al olvido en Internet. Google versus España*. Centro de Estudios Políticos y Constitucionales.

ROMEO CASABONA, C.M. (2006): “De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal”, en *El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales*. Editorial Comares, Granada.

SAINZ-CANTERO CAPARROS, J.E. (2015): “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. *Sistema de Derecho penal: Parte Especial*. 2.ª edición, Morillas Cuevas (Dir.). Dykinson, Madrid.

SANCHO LÓPEZ, M. (2020): *Derecho al olvido y big data: dos realidades convergentes*. Tirant Lo Blanch, Valencia.

SIMÓN CASTELLANO, P (2012): *El Régimen Constitucional del Derecho al Olvido Digital*. Tirant Lo Blanch, Valencia.