EL CUMPLIMIENTO DEL MANDATO CONSTITUCIONAL DE PROTECCIÓN DE LA INFANCIA Y LA ADOLESCENCIA EN EL ÁMBITO DE LAS REDES SOCIALES

Autor: Nuria Moreno Mariscal

Cuarto Curso de Derecho E1-JGP

Derecho Constitucional

Tutor: Francisco Valiente Martínez

Madrid

Junio 2022

Resumen:

El objetivo del presente trabajo es analizar si la protección jurídica que se proporciona, tanto a niños como a adolescentes en el ámbito de las redes sociales, es suficiente. Estas plataformas digitales han supuesto un notorio avance a lo largo de los años, pero, desafortunadamente también un peligro para aquellos colectivos inocentes y sin el suficiente conocimiento sobre lo que conlleva su exposición al resto de personas, así como su utilización. Profundizaré en el concepto y alcance de estos medios, así como las pérdidas de control que sufren los usuarios frente a terceros una vez que realizan el registro en dichas plataformas. Ejecutaré el estudio de la normativa aplicable y las diferentes formas de criminalidad que pueden desarrollarse digitalmente y que pueden llegar a condicionar el futuro, tanto personal como profesional de los menores.

Palabras clave: menores, redes sociales, privacidad, protección, infancia, adolescencia, internet.

Abstract:

The objective of this paper is to analyze if the legal protection provided, both to children and adolescents, in the field of social networks is sufficient. These digital platforms have represented a notable advance over the years but, unfortunately, they are also a danger for those innocent groups without sufficient knowledge about what their use entails for other people, as well as their use. I will delve into the concept and scope of these means as well as the loss of control suffered by users against third parties once they register with them. I will carry out the study of the applicable regulations and the different forms of criminality that can be developed digitally and that can condition the future, both personal and professional, of minors.

Key Words: *minors, social networks, privacy, protection, childhood, adolescence, internet.*

ABREVIATURAS:

CE: Constitución Española

S.: Siglo

Art.: Artículo

UE: Unión Europea

LOPDGDD: Ley Orgánica de protección de datos

RAE: Real Academia Española

INTECO: Instituto Nacional de Tecnologías de la Comunicación

Pág.: página

CP: Código Penal

LOPD: Ley Orgánica de Protección de Datos

AEPD: Agencia Española de Protección de Datos

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales regula el tratamiento de datos de carácter personal en España

LGCA: Ley General de la Comunicación Audiovisual

LSSI-CE: Ley de Servicios de la Sociedad de la Información

RGPD: Reglamento General de Protección de Datos

CC: Código Civil

TC: Tribunal Constitucional

ÍNDICE

I. INTRODUCCIÓN:

Este trabajo centra su atención en el análisis del cumplimiento del mandato constitucional de protección en el ámbito de las redes sociales, especialmente en lo relativo a la infancia y la adolescencia por el peligro al que se exponen en las diferentes plataformas de internet. Las redes sociales han transformado nuestro día a día.

Millones de usuarios optan por la utilización de este tipo de medios digitales para comunicarse de manera sencilla y sin requerir demasiado esfuerzo de manera diaria.
Las posibilidades que nos ofrece internet son infinitas, pero, como todo en la vida, también tiene una doble cara y esas ventajas pueden transformarse en inconvenientes si el conocimiento y la utilización no es el adecuado. Como afirma Josep Lluís Micó: *"muchas personas que parecen ser una cosa, en la red son otra"*. Y es que internet, nos ha habituado a que, todo aquello que solicitamos o que nos hace falta en un momento determinado, llegue a nosotros de manera inmediata.

Señala Shirley Cramer: *"Las redes sociales se han convertido en un espacio en el que formamos y construimos relaciones, damos forma a la identidad propia, nos expresamos y aprendemos sobre el mundo que nos rodea; está intrínsecamente ligado a la salud mental"* (González, 2021)**.**

Dada la importancia de la tecnología en la sociedad, la preocupación del desarrollo de niños y adolescentes cada vez es mayor. Hace años los jóvenes se reunían en el parque, en un centro comercial o incluso en el cine. Sin embargo, actualmente, han normalizado la comunicación a través de una pantalla y no en persona, disminuyendo así sus habilidades sociales.

Esta normalización se disparó durante el periodo de confinamiento al que tuvimos que hacer frente. Nunca antes habíamos tenido que permanecer en nuestras casas durante tantos meses de manera involuntaria y eso provocó que, tanto jóvenes como adultos, encontraran en las diferentes plataformas digitales los mayores aliados para mantener el contacto y sentir más cerca tanto a familiares como a amigos.

La consecuencia más notoria de esta sobreexposición digital, como indicó Joaquín González Cabrera, profesor de la Facultad de Educación de UNIR e Investigador Principal del grupo de ciber psicología de UNIR, ha sido la reducción que se ha producido en el contacto personal, especialmente en la infancia y la adolescencia, así como la disminución de actividades lúdicas y la práctica de deportes que han ocupado un lugar secundario en la sociedad promoviendo de esta manera el sedentarismo.

"Nueve de cada diez adolescentes tienen acceso a internet y siete de cada diez tienen móvil" como demuestran los estudios del Instituto Nacional de Estadística (Borondo, 2021). Existe una edad mínima para poder acceder a las redes sociales, pero este requisito, es frecuentemente incumplido. Por ello algunas de las plataformas más populares como WhatsApp o Instagram, han establecido alternativas especiales para los menores (Ferrer, 2021).

Es evidente que la tecnología nos ha abierto las puertas de numerosos servicios y nos ha proporcionado la ayuda que, sin ella no sería posible, pero internet es "una caja de sorpresas" y debemos conocer los peligros que esconde promoviendo la concienciación de las consecuencias que pueden llegar a sufrir los menores, repercusiones que pueden dañar su futuro, tanto personal como profesional.

II. METODOLOGÍA:

El objetivo principal de este trabajo ha sido la recopilación de información ya existente sobre la protección constitucional de la infancia y la adolescencia en el ámbito de las redes sociales. He analizado de manera crítica la información y los datos obtenidos llevando a cabo comparaciones entre las fuentes con el fin de poder responder a la pregunta en que se basa mi investigación: ¿es la protección jurídica de los menores de edad en las plataformas digitales suficiente?

Los pasos que he seguido han sido los siguientes:

1. Justificación de la revisión bibliográfica argumentando el porqué de la elaboración de dicha investigación.
2. Recopilación de fuentes mediante la búsqueda de artículos, libros o páginas web.
3. Evaluación y selección de la documentación más relevante.
4. Elaboración de la revisión bibliográfica desarrollando los resultados y conclusiones de mi trabajo así como utilizando el estilo de citación APA.

III. RÉGIMEN JURÍDICO DE LAS REDES SOCIALES

En primer lugar, es necesario aludir al concepto de red social para poder examinar la normativa vigente de las mismas. Debemos remitirnos a la denominación del Dictamen 5/2009 sobre redes sociales en línea[1].

Aunque en la LOPD no se haga una mención específica de las redes sociales, se alude a las mismas en el art. 2 de dicha ley[2]. Estas plataformas han tenido que adaptarse y modificar sus políticas de privacidad existentes debido a la aparición del Reglamento General de Protección de Datos (RGPD) europeo y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) para asegurar el respeto de los derechos de los internautas que hacen uso de las mismas.

Partiremos de la premisa de que todo usuario, ya sea personal o individual, que se registra y hace uso de la información que encuentra en las redes lo hace en un entorno "doméstico", lo cual no está sujeto a dicha ley (Consulting, 2012) . Esto se encuentra en el artículo 4[3] del reglamento de desarrollo de la LOPD.

[1] Dicho Dictamen asegura que*: "son plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes".*
[2] El artículo de dicha ley establece: *"se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".*
[3] El artículo 4 LOPD establece que dicho régimen no tomará parte en los *"ficheros y tratamientos realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas",* es decir en el seno familiar.

Para poder diferenciar cuando una actividad llevada a cabo en la red es personal o domestica deberemos hacer uso de lo expresado por la RGPD donde, con respecto a la Directiva 95/46, nos aporta una serie de concreciones afirmando que se considera una actividad personal[4] cuando *"no haya conexión alguna con una actividad profesional o personal"*.

Obligaciones de las redes sociales según la LOPD:

A nivel nacional y de forma concreta, las obligaciones que se exigen son las siguientes:

- Realizar un fichero incluyendo las actividades de tratamiento que se llevan a cabo.
- Habilitar un documento de seguridad con todas las medidas de seguridad.
- Notificar a los involucrados en el asunto de los derechos de los que disponen.
- Cumplimiento de los principios por parte del responsable del fichero.

(Grupo atico 34, 2021).

Los principios mencionados previamente que deben respetar y hacer efectivos los responsables de los ficheros se recogen del artículo 4 al 12 en esta Ley Orgánica:

PRINCIPIO DE CALIDAD DE DATOS:

Se puede denominar así mismo como el principio de proporcionalidad y, el requisito básico que encontramos, es que el objetivo de su creación debe corresponderse con el trato que reciben. Más específicamente si se utilizan para una finalidad diferente se deberá proceder a la supresión de los mismos[5].

PRINCIPIO DE INFORMACIÓN:

Los internautas que hacen uso de las redes sociales cotidianamente deben ser notificados y advertidos de los derechos de los que disponen, así como del tratamiento de sus datos.

[4] Con el correspondiente deber que tienen las autoridades de control de establecer los diferentes registros facilitando dichas actividades.

[5] Como sucedió en la STS 962/2018, 23 de Marzo 2018, en la cual se condenó a la demandada a ejecutar cuantos actos sean necesarios para cancelar los datos del actor en el fichero Badexcug.

PRINCIPIO DEL CONSENTIMIENTO[6]:

La intimidad es una cuestión esencial y de notoria relevancia en la actualidad y, por ello, es completamente necesario el consentimiento de los usuarios sin que este se considere implícito.

PRINCIPIO DE DATOS ESPECIALMENTE PROTEGIDOS Y DATOS DE SALUD[7]:

No está permitido el trato de este tipo de datos. Aquellos que implican una medida de seguridad especialmente elevada así como un consentimiento expreso por parte del individuo son los que versan sobre la ideología, la religión, las diversas creencias así como los que se basan en el origen racial. Los datos de salud los encontramos en el art. 5 LOPD.

PRINCIPIO DE SEGURIDAD

Recogiendo las medidas que deben ser adoptadas por los responsables.

PRINCIPIO DE DEBER DE SECRETO:

El responsable del fichero debe guardar el secreto[8] y la confidencialidad una vez se dé por terminado el tratamiento de los datos.

PRINCIPIO DE COMUNICACIÓN:

En este último principio recogido en dicha Ley Orgánica se muestran los contextos y las condiciones para optar a la posibilidad de la cesión de datos personales.

Los derechos más notables son los conocidos por la abreviatura ARCO[9] que solo pueden ser ejercidos por el titular de los datos o por su representante legal. Están recogidos tanto en el RGPD[10] como en la LOPDGDD y son los siguientes:

DERECHO DE ACCESO:

[6] Principio recogido en el artículo 6 LOPD.

[7] El Tribunal Constitucional, en su Sentencia 292/2000, de 30 de Noviembre de 2000 (BOE de 4 de Enero de 2001).

[8] Sentencia administrativo nº 5/2022, Tribunal Superior de Justicia de País Vasco, Sala de lo Contencioso, Sección 2, Rec 260/2019 de 11 de Enero de 2022.

[9] Cuyo objetivo principal es permitir que las personas físicas tengan un mayor control de sus datos personales.

[10] Concretamente en el Título III LOPD.

Se trata del derecho a obtener información personal sobre uno mismo sin necesidad de un motivo justificado. El responsable del fichero deberá dar una contestación a la solicitud en el plazo de un mes desde la recepción de la misma.

DERECHO DE RECTIFICACIÓN:

Es un derecho basado en la corrección o eliminación de cualquier tipo de dato erróneo sobre el usuario de la plataforma digital. El plazo para este derecho es de 10 días hábiles en los que deberá recibirse una contestación a la solicitud, ya sea negativa o positiva.

DERECHO DE CANCELACIÓN:

Aquella información inadecuada o excesiva podrá ser suprimida por el titular de la misma. La solicitud debe ser atendida siempre. Su plazo es de 10 días hábiles.

DERECHO DE OPOSICIÓN:

Consiste en permitir al usuario que el tratamiento de sus datos no se lleve a cabo cuando *"se trate de ficheros de prospección comerciales o tengan la finalidad de adoptar decisiones referidas al interesado basadas únicamente en el tratamiento automatizado de sus datos*[11]*".*

IV. LA PRIVACIDAD DEL MENOR EN INTERNET

4.1. La intimidad informática de los menores y su protección

La importancia que ha cobrado internet en nuestras vidas ha roto toda clase de barreras para las posibles intromisiones ilegítimas en la vida de las personas y ello ha hecho que la protección de los individuos en la red se haya convertido en una exigencia prioritaria, en especial la protección de los menores.

El punto de partida se encuentra en el momento en que las redes sociales surgieron con la intención de mantener el contacto con personas que, los usuarios habían conocido

[11] Como sucedió en la Sentencia de la Audiencia Nacional 5239/2014, 30 de diciembre 2014.

previamente y con los que no querían perder relación. Hemos de resaltar que las mismas no fueron pensadas ni, para niños, ni para adultos, sino para los menores de edad y, de

Ahí que la edad mínima requerida para acceder a ellas sea de catorce años[12] (Davara Fernández de Marcos, 2016).

La utilización habitual de internet ha universalizado derechos como la libertad de información o la libertad de expresión[13] entre otros. Sin embargo, eso ha generado graves vulneraciones de muchos otros como el derecho a la intimidad de las personas o la protección de datos personales, derechos intrínsecos al círculo de la privacidad (Alcón y Platero 2016).

Tanto a nivel internacional como en nuestro ordenamiento han surgido nuevos derechos fundamentales que tratan de velar por la dignidad y el respeto humano como el derecho al olvido o aquellos recogidos en el art. 18.1 de nuestra Constitución entre otros.

Sin embargo, los avances tecnológicos en muchas ocasiones escapan de nuestro control y es ahí cuando surgen los peligros y los actos delictivos. LOPEZ ORTEGA afirmó que: *"ningún sentido tiene reconocer el derecho al control sobre los datos personales si esos datos ya no circulan en redes civiles cerradas sobre las que se pueda imponer un estricto control"*.

De acuerdo con la definición de la Real Academia Española de la Lengua la privacidad está constituida por el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. A medida que transcurren los años son más los niños que nacen

"con la pantalla debajo del brazo" tal y como afirmó TRONCOSO REIGADA en la Conferencia Europea de Protección de Datos celebrada en Edimburgo el 24 de abril de 2009 denominando a todas aquellas personas nacidas después de 1995 "digital babies o digital natives " (Gil Antón A. , 2013a).

[12] Estando prohibido el registro en estas plataformas sin el consentimiento previo del tutor legal del menor.
[13] Dichos derechos comprenden la posibilidad que tiene el individuo, sin estar sujeto a censura, de divulgación e investigación a través de cualquier medio.

Para su protección frente a terceros en internet son muchos los que abogan por limitar a este colectivo su acceso a la web, pero realmente esa no es la óptima solución puesto que mantenerlos al margen solo generaría en ellos una mayor curiosidad por adentrarse en el mundo tecnológico (Gil Antón A. M., La Privacidad del Menor en Internet , 2013a).

Por ello no se trata de aislarlos del mundo tecnológico sino de tratar de cambiar las actitudes que mantienen los jóvenes y adolescentes en las redes sociales ya que la misma puede condicionar sus posibilidades futuras.

Sin embargo, ni los menores son capaces de reconocer por ellos mismos las contingencias de internet para su privacidad. Sin embargo, se han promovido numerosas iniciativas para que los peligros de la web para este colectivo sean mínimos, aunque ello suponga un gran resto especialmente en los casos en los que el propio menor cede su consentimiento (Gil Antón A. M., La Privacidad del Menor en Internet, 2013b).

4.2. Impedimentos de los medios jurídicos para la protección de los derechos de los internautas menores

Como afirmó Tim Berners Lee[14] *"No sabía que iba a pasar con la Red, pero sabía que quería que fuese un espacio universal. Sabía desde el principio que era muy importante que no se dejase relegado a ningún círculo en particular".*

Dicho esto, tratar de controlar el acceso a la web basándonos en la edad de cada individuo parece un acto contrario a la razón por la que fue creada Internet, como un espacio libre sin obstáculos ni impedimentos (Balderas Blanco, 2015).

Hoy en día, la comunicación se encauza cada vez más a menudo a través de la tecnología, sector en el que destacan los menores y, por ello, debemos estimar si la regulación, tanto a nivel nacional como internacional, es la correcta. Si analizamos los recursos que nuestro Ordenamiento Jurídico nos proporciona puede parecer que nos encontramos perfectamente protegidos por los mismos, sin embargo, si nos centramos en clausulas

[14] Quién es considerado como El Padre de Internet.

específicas nos damos cuenta de que estas son completamente abiertas y difusas (Gil Antón A. M., La Privacidad del Menor en Internet, 2013c).

Debemos destacar la Ley 7/2010 de 31 de marzo, General de la Comunicación Audiovisual (LGCA), la cual se comprometió fervientemente a la protección de los menores en el ámbito tecnológico, una decisión aparentemente cabal y acertada, pero, que sin embargo, resulta preocupante ya que tras un año de vigencia no se ha constituido una autoridad encargada de asegurar su cumplimiento (Fuente Cobo).

En España, en el año 2009, la Agencia de Protección de Datos tomó la iniciativa tratando de subsanar la problemática que presentaban numerosos aspectos que quedaban al descubierto en el ámbito de la privacidad (Herce Ruiz, Aspectos Jurídicos Sobre la Privacidad en las Redes Sociales, 2012a).

Como afirmó Antonio Troncoso Reigada[15]: *"la privacidad no sólo trata del respeto a nuestros datos personales sino también del que debemos de tener por la información relativa a los demás"*.

Son las entidades las que deben hacerse cargo de garantizar la seguridad informática de todos los usuarios, especialmente de los menores, de tal manera que nadie pueda tener la posibilidad de acceder a información confidencial de otros individuos salvaguardando la privacidad de todos los internautas (Herce Ruiz, Aspectos Jurídicos sobre la Privacidad en las Redes Sociales, 2012b).

4.3 Iniciativas de protección de la privacidad de los menores en internet

"Internet fue diseñado para adultos, pero los niños y los jóvenes lo utilizan cada vez más, y la tecnología digital afecta cada vez más sus vidas y su futuro. Por ello, las políticas, las prácticas y los productos digitales deberían reflejar mejor las necesidades, las perspectivas y las opiniones de los niños" (Unicef, 2017).

[15] Director de la Agencia de Protección de Datos de la Comunidad de Madrid desde el año 2001 hasta el 2010.

La protección del menor en Internet es uno de los compromisos establecidos tanto por el sistema educativo como por el sistema judicial.

En primer lugar, debemos remontarnos a la 30ª Conferencia Internacional de la Privacidad en el año 2008 donde fue aprobada la Resolución sobre la protección de la Privacidad en las Redes Sociales, así como el Referéndum de Roma y el I Seminario euro-Iberoamericano de Protección de Datos en Colombia en los cuales "los menores y las tecnologías" fue el tema clave a tratar (Gil Antón A. M., La Privacidad del Menor en Internet, 2013d).

La Agencia Española de Protección de Datos ha sido consciente, a lo largo de numerosos años, de la realidad con el mundo virtual y de los numerosos riesgos a los que se enfrentan los menores al hacer un uso reiterado e irresponsable de la red. Por ello, tomó la iniciativa de garantizar su protección mediante la puesta en acción de medidas preventivas y de concienciación de los mismos (Intef, s.f.).

A nivel nacional diversas administraciones Públicas han sido promotoras de una serie de iniciativas con el principal objetivo de concienciación y sensibilización de la población. Entre ellas podemos destacar las siguientes: (Junta de Castilla y León, s.f.).

- *Proyecto Secukid*. Iniciativa promovida por AETICAL dentro del programa Ded@alo, INTECO y Pantallas Amigas. Se basa en un juego de inteligencia para dispositivos móviles con cinco niveles: virus, troyanos y gusanos, programas espía, ciberbullying y grooming.
- *Wild Web Woods*[16] promovida por el Consejo de Europa. Consiste en un juego para los menores mostrándoles cómo convertirse en unos internautas prudentes recibiendo información de seguridad en la Red.
- *Pantallas Amigas*[17]. Iniciativa de EDEX e Integral de Medios, con recursos educativos para un uso de la web para menores.

Por otro lado, a nivel internacional debemos destacar que existen una serie de Recomendaciones basadas en el uso de Internet por menores creadas por diversas

[16] El juego consiste en el reto de llegar a "la ciudad electrónica" evitando los riesgos de la red.
[17] Iniciativa que nació en el año 2004 con el objetivo de ofrecer un uso seguro y saludable de Internet.

instituciones. Entre ellas podemos mencionar el Programa Comunitario del Parlamento Europeo cuyo fin es disminuir la existencia de contenidos ilícitos, así como el Proyecto Dadus en Portugal y el Proyecto Prometeo. A todo ello tenemos que añadir la iniciativa promovida por la propia Comisión Europea fundamentada en un nuevo marco jurídico con el objetivo de la protección de los datos personales de los individuos en Internet. La creación de este nuevo marco jurídico surge como consecuencia de la Directiva 46/95/CE que ha dado lugar a la normativa vigente.

Este tipo de iniciativas impulsadas, tanto a nivel nacional como internacional, ha competido tanto a los Estados como a los representantes de la sociedad y a los proveedores de servicios en la red[18] (Gil Antón A. , 2013b).

V. CONCEPTO DE PROTECCIÓN DE DATOS Y SU MARCO NORMATIVO

La irrefutable necesidad de la protección de nuestros datos se basa en la inmensa cantidad de información compartida relacionada con cada uno de nosotros, ya sea referida a nuestra vida privada o pública, y por esta razón es preciso que verse un control de la misma.

Es aquí donde aparece la protección de datos. Este es el proceso por el que se ampara cualquier tipo de información de los individuos ante acciones ilegitimas por parte de terceros así como es el derecho inherente a todos nosotros el cual se consagró en la STC 290/2000 de 30 de noviembre.

La Protección de datos es un derecho fundamental con eficacia directa recogido en la Constitución Española. Este derecho se encuentra entre los artículos 14 y 19 del Capítulo 2º de la misma. Para que quede completamente protegido cuenta con los requisitos de regulación por parte de una Ley Orgánica así como la necesidad de recabar una mayoría absoluta de votos en el Congreso de los Diputados[19] (Esténtor, s.f.).

El derecho a la protección de datos deriva del artículo 18. 4 de nuestra Constitución Española de 1979 donde se afirma que el uso de información será restringido por la ley

[18] Profesionales cuya labor consiste en proporcionar a los usuarios la suscripción o el servicio web como por ejemplo el acceso a internet.

[19] Circunstancia en la que una proposición o una votación alcanza más de la mitad de votos, es decir, cuando se obtiene el voto favorable de la mayoría de sus integrantes.

para poder asegurar y afianzar a los ciudadanos tanto la intimidad como el pleno ejercicio de otros de sus derechos.

La normativa vigente de este derecho la encontramos formada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal que entró en vigor el 14 de enero del año 2000. Esta Ley trajo consigo la modificación o variación a nuestro Ordenamiento de la Directiva 95/46/CE que finalmente fue sustituida por la Ley Orgánica 15/1999 que es actualmente la denominada LOPD (BOE núm. 298, 14 de diciembre).

La aplicación de la LOPD conlleva y requiere la protección de la información en el progreso de todo tipo de diligencias. Como ya hemos hecho un mayor hincapié previamente, esta ley incluye una serie tanto de obligaciones como de principios con el objetivo de proporcionar y ofrecer a los usuarios el adecuado tratamiento y gestión de sus datos personales.

5.1 El menor como sujeto especialmente protegido

Internet ha conseguido crear un mundo más conectado no obstante no lo ha hecho un mundo más seguro. El robustecimiento que tienen las tecnologías en la actualidad es innegable así como la indiscutible necesidad de enseñar, controlar y prever los efectos dañinos de las redes en los colectivos más ignorantes en relación a esta cuestión.

En materia de protección de datos ya se han llevado a cabo diversas iniciativas por parte de la Agencia de Protección de Datos que posteriormente explicaremos de manera más específica.

En definitiva la falta de madurez y de conocimiento de los menores de edad así como su consideración de individuos vulnerables ha causado que su privacidad y protección sea uno de los objetivos más primordiales en la actualidad.

5.2 El consentimiento del menor para el tratamiento de sus datos personales

Con el artículo 7 de la LOPDGDD ha sido establecido en España el término de la edad de 14 años para el consentimiento en un menor de edad. De esta manera, un niño que alcance dicha edad podrá otorgarlo el mismo en relación al tratamiento de sus datos pero, un menor que no alcance dicho límite no poseerá dicha libertad y deberán ser sus responsables quienes lo hagan (Del Águila, 2018).

Atendiendo así mismo al artículo 4.11 RGPD, el consentimiento es una declaración por parte de un individuo que debe ser calificada como libre, concreta, informada e inequívoca. Este podrá retraer su consentimiento cuando lo considere oportuno. Cabe destacar que, en los centros docentes o cualquier institución en la que haya menores involucrados deberá asegurarse de manera inexcusable el interés y protección de los mismos así como la garantía de sus derechos. (AEPD)

Un aspecto novedoso que se introdujo en la LODGDD fue la garantía de los derechos digitales con especial mención a los menores. Dicha garantía se encuentra recogida en dos artículos: el artículo 83 de dicha ley, el cual recoge el derecho a la educación, garantizado en la Constitución pero, en relación a la sociedad digital tratando de persuadir a los niños de los peligros a los que pueden llegar a hacer frente en la web así como la consideración de su privacidad. Otra figura destacable es el artículo 84 de la misma ley que se basa en el establecimiento de la protección de los menores en el área digital como un derecho y, a su vez, como una obligación asegurando con la diligencia adecuada la seguridad de estos (Beloki, 2021).

Por lo tanto, podemos afirmar que un menor de catorce años no estará legitimado para dar su consentimiento pero, sin embargo, aquellos que se encuentren entre dicha edad y la mayoría de edad podrán proporcionarlo lícitamente a no ser que haya una ley que establezca lo contrario. Será necesaria una especial atención en el tratamiento de datos de los menores de edad y así lo reclama la APED exigiendo un mayor vigor ya que nos referimos a un colectivo muy vulnerable que aún no se encuentra formado en su totalidad.

5.3 El papel de los padres frente al menor de edad en el uso de las redes sociales

5.3.1 Conflicto entre el ejercicio de la patria potestad de los padres frente al derecho a la intimidad del menor

La cuestión a tratar es la ponderación de si prevalece el derecho a la intimidad y secreto de las comunicaciones[20] de los hijos menores o si, por el contrario, es primordial el deber que tienen los padres de ejercer la patria potestad[21] que les corresponde[22].

Cuando un menor no alcanza la edad de catorce años no encontramos dificultad alguna puesto que los padres no necesitan consentimiento alguno por parte de su hijo sin embargo, el conflicto aparece cuando alcanzan dicha edad y se niegan a conceder el acceso a sus datos (Sesma Goñi, 2018).

En este sentido, resulta interesante la Sentencia de 10 de diciembre de 2015 (SP/SENT/840818) en la cual la Sala Segunda, de lo Penal, del Tribunal Supremo, decidió admitir las pruebas y evidencias presentadas por una madre quién las obtuvo mediante el acceso a la cuenta de Facebook de su hija con el propósito de demostrar que la menor estaba siendo víctima de acoso sexual a través de dicha plataforma social. El Tribunal Supremo alegó que se trataba de la figura materna y no de cualquier otro particular. Así mismo se trataba de una actividad delictiva no agotada y era necesario acabar con ella (García, 2016).

En conclusión, de la sentencia podemos aclarecer que los padres no pueden entrar en las cuentas de redes sociales de sus hijos de manera infundada y en vano violando la

[20] Derechos que se encuentran recogidos en el Título primero. De los derechos y deberes fundamentales de nuestra Constitución. Más concretamente en el capítulo segundo, sección 1ª, artículo 18.

[21] El ejercicio de la patria potestad se encuentra regulado en los arts. 156 y 154 CC, cuya actual redacción establecida por la Ley 26/2015 establece que *: "La patria potestad, como responsabilidad parental, se ejercerá siempre en interés de los hijos, de acuerdo con su personalidad, y con respeto a sus derechos, su integridad física y mental".*

[22] Debemos destacar la Ley Orgánica de Protección Jurídica del Menor 1/1996 reconoce en su art. 4.1 que*: "Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen".*

intimidad de los mismos. Por ello se deberá realizar una ponderación de intereses analizando las circunstancias y si son de apremiante necesidad.

Frente a todas las posibles situaciones debemos mantener el sentido común y buscar una solución proporcionada y el equilibrio idóneo entre no intervenir bajo ningún concepto y controlar a los menores constantemente. Contamos con un amplio abanico de opciones respetando su espacio personal pero velando por su interés y protección.

5.3.2 Conflicto en el tratamiento de los datos de un menor de edad por parte de padres separados

La cuestión suscitada en este caso es la manera de solucionar la problemática que surge si los progenitores están separados y uno de ellos quiere publicar contenido de su hijo en la web. Como ya hemos mencionado previamente solo analizaremos los casos que afecten a menor de catorce años donde el consentimiento es innegable.

Para resolver la misma debemos remitirnos al artículo 13 RDLOPD donde se especifica que será indispensable el consentimiento de ambas parte para compartir información acerca del menor en una plataforma digital. También se especifica que si no hay un acuerdo por parte de los progenitores y el hijo es mayor de doce años con capacidad suficiente podrá ser el mismo quien tome la decisión (BOE núm.17, 19 de enero).

En relación a este tema me gustaría destacar la Sentencia, dictada el día 4 de junio de 2015, por la Sección 1. ª De la Ilma. Audiencia Provincial de Pontevedra en la cual se presenta un caso de procedimiento de divorcio en el que el padre quería publicar una imagen de su hijo menor en la red social Facebook. La madre, quien poseía la custodia del menor, formuló un recurso de apelación alegando que con el fin de preservar la intimidad de su hijo no consentía la publicación de dicho contenido. Finalmente la Audiencia Provincial de Pontevedra concluyó que, atendiendo al Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal era indispensable el consentimiento expreso de ambos progenitores para la difusión de dicha imagen ya que el hijo no alcanzaba la edad de 14 años (Mateo Bueno, 2014).

De la misma manera la Audiencia Provincial de Barcelona, en la Sentencia de 25 de abril de 2017, con una situación similar a la mencionada previamente en la anterior sentencia se declara que, en el caso de la publicación del contenido con un consentimiento unilateral por parte de un solo progenitor, será declarado contrario al ordenamiento jurídico (Iberley, 2017)

En definitiva, en el supuesto de padres separados, ambos conservando la patria potestad del menor, será el juez quien tome la decisión si estos no consiguen alcanzar un acuerdo.

VI. NUEVAS FORMAS DE CRIMINALIDAD EN INTERNET

6.1 El sexting y el grooming

La evolución de la tecnología avanza en forma vertiginosa, y estamos llamados a ajustarnos a ese cambio, pero sin perder los valores éticos y morales[23].

A causa de la pandemia del Coronavirus a la que hemos tenido que hacer frente las redes sociales se han convertido en una dinámica utilizada por numerosos individuos para satisfacer sus necesidades sexuales. El uso incorrecto de la web en una etapa de vulnerabilidad como es la adolescencia puede acarrear graves consecuencias que pueden llegar a derivar en acoso escolar a través del ciberbullying o ciberacoso.
El continuo uso de las tecnologías ha supuesto la aparición de nuevas formas de criminalidad, maneras de cometer un delito a través de Internet. Entre estas vías de criminalidad encontramos "el sexting" y "el grooming".

El sexting es definido como: "el envío, especialmente a través del celular, de fotografías y vídeos con contenido de cierto nivel sexual tomados o grabados por el protagonista de los mismos" (Ayala, 2018).

[23] Save the children determina que:
"Es esencial tener en cuenta que especialmente en el online grooming, el engaño es lento y no hay consentimiento del niño o niña, no son conscientes de lo que ocurre y no tienen las herramientas adecuadas para defenderse, nunca podrá ser culpa de ellos. Se trata de un proceso[23] en el que se produce un vínculo de confianza entre la víctima y el acosador".

Este delito se encuentra tipificado en nuestro Código Penal por la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, más específicamente en el artículo 197.7[24].

El delito cometido, para ser considerado sexting, debe estar conformado por una serie de elementos como la difusión o revelación de imágenes de contenido íntimo y personal de la propia persona sin ningún tipo de autorización, el afecto de forma grave y notoria de su intimidad y que dicho material haya sido obtenido en el propio domicilio de la víctima o en cualquier otro lugar privado de la misma.

Lo característico de este tipo de delito es el consentimiento de la grabación, pero no en su posterior difusión a través de las plataformas digitales como WhatsApp, YouTube o Skype entre otras (Rojas, 2017).

Aunque el sexting no es considerado un tipo de ciberacoso puede llegar a derivar en formas de ciberacoso como pueden ser el grooming o la sextorsión. El principal problema está en la pérdida de control del contenido una vez enviado ya que el receptor puede difundirlas sin el consentimiento previo de quien se lo ha enviado, su dispositivo puede ser hackeado y puede ser objeto de publicación en la web de forma pública sin que la persona afectada pueda hacer algo al respecto para evitarlo (Anónimo, Cómo prevenir el Sexting en Redes Sociales, 2020).

En relación con el grooming podemos definirlo como: "El grooming es el acoso y abuso sexual online, son formas delictivas de acoso que implican a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual" (Anónimo, 2019).

Según el estudio llevado a cabo por Save The Children esta forma de ciberacoso es, actualmente, más común de lo que nos imaginamos. Tras realizar la encuesta se ha

[24]Este artículo recoge esta nueva figura delictiva en los siguientes términos: *"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".*

confirmado que: "*Uno de cada cinco de los encuestados ha sufrido este tipo de acoso y el 15% en más de una ocasión. De media, la primera vez que sufrieron esta violencia fue con 15 años".*

Existen una serie de etapas o fases que son seguidas habitualmente por el agresor. Como ya hemos mencionado previamente, las victimas suelen ser jóvenes y adolescentes, un colectivo muy atado a Internet y sin el suficiente conocimiento de los riesgos que pueden llegar a sufrir si no hacen un uso correcto de las redes sociales.

La primera de estas fases se basa en tratar de crear un vínculo con la víctima, es decir, intentar ganarse la confianza del menor generalmente haciéndose pasar por otra persona de su edad y mostrando preocupación, empatía e interés por sus asuntos personales. Una vez el menor "ha caído en la trampa" y confía en su agresor este trata de apartarle de su círculo de personas más cercano, de su familia, de sus amigos convenciéndole de que debe mantener su relación, ya sea afectiva o de amistad, en completo secreto. Antes de introducir en sus conversaciones la temática sexual, el acosar se asegura de evitar todo tipo de riesgos, es decir, eliminar las formas en que pueda ser descubierto. Cuando considera que tiene "vía libre" para conseguir su objetivo comienza a iniciar conversaciones sexuales con su víctima, de manera que esta finalmente normalice esa clase de diálogos a través de la web. Llegados a ese punto el criminal pasa a su última fase en la cual se encuentra el objetivo del grooming y es manipular, chantajear o incluso coaccionar a la víctima para que esta acepte enviarle contenido sexual (Grooming, qué es, cómo detectarlo y prevenirlo, 2022).

Evitar este tipo de prácticas de acoso y abuso sexual es, afortunadamente, sencillo mediante unas medidas de prevención y seguridad de navegación.
Los padres desempeñan el papel principal en estas ocasiones, deben concienciar a sus hijos de las consecuencias fatales que pueden sufrir si no utilizan la red de una manera madura y correcta, así como el dialogo abierto en el seno familiar es de gran importante para que los menores sientan la cercanía de sus familiares y no el miedo ante las posibles reacciones que puedan tener sus padres si tratan de pedirles ayuda cuando están sufriendo este tipo de acoso a través de Internet.

6.2. El ciberbullying

Lo más importante para que exista el ciberbullying es la involucración de dos menores en ambos extremos del ataque puesto que si una de las partes está formada por un adulto esto derivaría en ciberacoso.
Según el Estudio sobre hábitos seguros en el uso de las TIC por los menores publicado por el INTECO en marzo de 2009 el ciberbullying se define como acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños (2009).

Habitualmente los casos de ciberbullying muestran tres elementos comunes en todos ellos. Estamos hablando del anonimato, de roles imaginarios y perfiles falsos en la web y la no percepción del daño causado con las acciones cometidas. El ciberbullying es un hostigamiento del acosador a su víctima tanto en su contexto social como en su contexto digital, debe estar presente en ambos.

Pero, realmente, ¿Cuál es el origen de este hostigamiento? ¿Qué ha hecho la víctima para sufrirlo precisamente ella y no otra persona? Habitualmente, el origen del ciberbullying tiene lugar en una situación de inferioridad que siente el mismo agresor quien considera que humillando y ridiculizando a su víctima pondrá fin a su frustración y complejos.

Según Parry Aftab[25] : “el ciberacoso es el riesgo más frecuente para los niños" (Ambrojo, 2006). Es muy frecuente que aquel menor que ha sufrido ciberacoso sea su motivo para llevarlo a cabo con otras personas, pero, en ese caso, intercambiando su papel al de agresor. Lo más preocupante es que, habitualmente, el acosador no es consciente ni se ve como un abusador (2018).

El este tipo de abuso a través de la red la victima que lo sufre siente una mayor indefensión que en otros tipos de bullying puesto que el ataque hacia su persona le puede llegar en cualquier momento y en cualquier lugar, siendo innecesaria la presencia física y, además, al realizarse a través de la web, suele llevarse a cabo de manera anónima sin la revelación de la identidad del agresor.

[25] Abogada especializada en privacidad y seguridad en Internet.

No existe un solo tipo de ciberbullying, sino que hay un amplio abanico de formas en las que lo puede sufrir la víctima como el grooming o el sexting.

6.3 Hostigamiento o stalking

Este delito fue introducido por la Ley Orgánica 1/2015, de 30 de marzo en la que se recoge nuevos tipos penales como el acoso ilegítimo, hostigamiento o stalking regulados en el artículo 172 ter del Código Penal.

Este artículo establece que un individuo que realice una conducta acosadora de un modo habitual y reiterado sin ningún tipo de consentimiento, llevará consigo una pena de prisión de tres meses a dos años así como una multa de seis a veinticuatro meses. Todo ello si el desarrollo de la vida de esta tercera persona se ve alterado de forma notoria. Las conductas que se recogen en el mismo y las cuales están penadas son la vigilancia y búsqueda de manera física, el intento de obtener un contacto por cualquier medio o persona, un uso no autorizado de los datos personales e íntimos con una finalidad lucrativa así como la perturbación de su libertad o patrimonio o de una persona de su círculo cercano
(Ley Orgánica, de 23 de noviembre, del Código Penal).

El bien jurídico protegido[26] es la libertad, la seguridad esto es el derecho de sosiego y la tranquilidad de la persona.

Para que este tipo de delito sea punible, se deben dar cuatro modalidades de conductas. La vigilancia o búsqueda reiterada de la víctima ya sea de manera física o a través de cualquier dispositivo electrónico, tratar de establecer comunicación con ella, así como atentar contra su libertad o patrimonio o hacer un uso indebido de sus datos personales.

[26] Cuando hablamos de un bien jurídico protegido hacemos referencia a cualquier valor de la vida que está protegido por la ley. Puede ser tangible o intangible y merece una garantía real para evitar las vulneraciones por parte de un tercero.

Este tipo de conductas deben ser graves y constantes, es decir, que el agresor lo realice de manera habitual. Este tipo de delito es frecuente en la violencia de género, lo cual supone un agravante para la pena establecida (Roig Rosselló, 2020).

Esta figura delictiva es relativamente nueva en nuestro ordenamiento jurídico y por ello la jurisprudencia es escasa, pero debemos recordar un caso recogido en la STS número 324/2017, de 8 de mayo que presenta cuatro episodios. El primero de ellos trata una serie de llamadas telefónicas. El segundo sucede al día siguiente en el que el agresor comete una tentativa de entrada en el domicilio de la víctima. Y una semana más tarde el sujeto activo se acerca a la víctima en un centro al cual ambos individuos acudían con frecuencia. Sin embargo, el fallo fue la no concurrencia de los elementos típicos de Stalking a la víctima porque, aunque los actos fueron reiterados y próximos cronológicamente, presentan una morfología muy diferente.

De esta manera las acciones de naturaleza muy diversa o que sean llevadas a cabo en días concretos y puntuales pueden llegar a impedir la consideración del patrón de este tipo de acoso.

6.4 Injurias y calumnias

Los delitos contra el honor son actos ilícitos que atentan contra el prestigio o dignidad de la persona, entre los que encontramos las calumnias y las injurias.

En primer lugar, la calumnia hace referencia a la imputación de un delito hecho con conciencia de su falsedad o temerario desprecio hacia la verdad, se encuentra tipificado en el artículo 205 de nuestro Código Penal[27].

[27] Este artículo establece que: "*Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad*".

Por otra parte, la injuria es definida como la acción que se comete con intencionalidad de lesionar la dignidad de la otra persona, atentando contra su propia estimación, delito tipificado en el artículo 208 CP[28].

A la hora de determinar esta serie de delitos hay que hacer un análisis del supuesto para determinar si se está violando el derecho al honor, a la intimidad y a la propia imagen del afectado, derecho fundamental recogido en nuestra Constitución (Rojas, 2017).

Los principales elementos característicos del tipo básico de estos dos delitos son la existencia de un hecho tipificado y constituido de delito, que dicha imputación sea falsa y se realice con una actitud voluntaria de desprecio y de manera específica. El delito debe ser público hacia una persona concreta y que el autor del mismo sea consciente de que el acto que está llevando a cabo es ofensivo para un tercero.

Sin embargo, debemos mencionar que si el autor acusado de cometer un delito de calumnia demuestra el hecho criminal quedara exento de pena alguna. Cuando se realice la calumnia con publicidad de cualquier tipo será un agravante para la condena establecida por ello.
El contenido de las injurias[29] debe ser objetivo y con un grave carácter ofensivo en el que debe estar presente el dolo y una conducta voluntaria de menosprecio y deshonra hacia el sujeto pasivo. Este delito también se agrava si el elemento publicitario está presente en el delito cometido (Gersonvidal, 2022).

En ciertas ocasiones el derecho al honor puede entrar en conflicto con otro derecho fundamental, la libertad de expresión[30].

Estos dos derechos poseen un grado de protección equivalente, pero cuando las ideas expresadas atenten el honor de otra persona se genera un conflicto entre ambos derechos

[28] La injuria es definida como: "*la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación*".

[29] Tras la reforma que sufrió el Código Penal en el año 2015 las injurias leves pasar a ser consideradas un delito leve, no son penalmente punibles.
[30] En el artículo 20.1. de nuestra Constitución Española se expresa lo siguiente*: "1. Se reconocen y protegen los derechos: a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción".*

y será el juez el responsable de tomar la decisión sobre qué derecho prevalece por encima del otro.

6.5 Estafas informáticas

Este delito se encuentra regulado en el artículo 248.2 de nuestro Código Penal, dentro de los delitos contra el patrimonio y el orden socioeconómico:

Se acusa de estafa a aquellos individuos que, de manera suficiente y con ánimo de obtener algo a cambio, traten de inducir a un tercero a la comisión de un acto contraproducente y nocivo para ellos. También se especifica una serie de hechos que conllevan la acusación de delito de estafa: cualquier tipo de manipulación informática como una trasferencia, la creación de programas informáticos con el fin de la comisión de este delito así como el uso de tarjetas o similares para causar un detrimento en su titular. (Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal).

El bien jurídico protegido es el patrimonio ajeno puesto que mediante este delito se pretende obtener el acceso a los datos bancarios de la víctima. Las estafas informáticas se basan principalmente en tres conductas: la manipulación del sistema informático para causar un perjuicio a la víctima, la creación de programas informáticos con el fin de cometer estafas y la utilización de tarjetas bancarias para llevar a cabo operaciones mediante trasferencias (Arjona, 2021).

Las estafas más comunes son:

1. Pishing: se trata de una técnica de ciberdelincuencia que consiste en la manipulación de las victimas mediante el engaño, fraude o timo de tal manera que ellas mismas revelen su información personal. Sin dar importancia al medio por el que se lleven a cabo todos siguen los mismos pasos. El atacante envía a su víctima un enlace, un archivo adjunto o incluso la realización de un pago para así obtener sus datos personales. Todo ello genera pérdidas patrimoniales, pero también pérdida de confianza en los demás, siendo esa recuperación más lenta. Existen diferentes tipos de pishing: por correo electrónico, por sitio web, el vishing o lo que se conoce como el pishing mediante llamadas telefónicas,

mediante SMS y por último a través de las redes sociales. Cabe destacar que se han presenciado a lo largo de los años diversos casos basados en este tipo de estafa de gran notoriedad. En primer lugar, el que tuvo lugar durante el Mundial del año 2018 donde numerosas personas aprovecharon la ocasión para ofrecer a las víctimas tanto entradas gratis como ofertas de alojamiento extraordinarias. Nombrar así la conocida operación *Phish Phry* en el año 2007, la cual se convirtió en la operación de mayor repercusión llevada a cabo por el FBI. Se trataba de una organización de phishing que persuadía y engañaba a las víctimas para obtener datos bancarios a través tanto de correos electrónicos como de sitios web falsificados, con ello los atacantes lograron transferir 1,5 millones de dólares (Belcic, 2020).

2. SIM swapping: esta estafa informática consiste en realizar una duplicación de la tarjeta SIM de la víctima. Con ello toman el control de su teléfono móvil teniendo en su posesión toda la información que contiene el mismo. Lo imprescindible es obtener los datos personales así como los códigos del banco online para obtener documentos de identidad falsos que les permitan solicitar una segunda tarjeta anulado la auténtica y original y así poder realizar las trasferencias que consideren (Lleida, 2021).

3. Redes sociales: es relevante mencionar que este tipo de fraude ha incrementado a raíz de la pandemia del Corona Virus debido a la publicación de anuncios falsos basados en pruebas o incluso en tratamientos de la COVID-19. También se han llegado a enviar mensajes privados con enlaces falsos para ayudas o subvenciones por la pandemia (AARP, 2021) . Debido al tiempo que pasan los adolescentes en las redes sociales los estafadores les tienen en el punto de mira. El método más común que llevan a cabo es el envío de enlaces que dirigen a un sitio web malicioso así como la invitación a sorteos o concursos pero que lo único que pretenden es la sustracción de información confidencial de la víctima (Owaida, 2021).

4. Compras online: nuestros hábitos de compra han cambiado mucho en los últimos diez años, antiguamente nuestras compras eran mayoritariamente en tiendas físicas, sin embargo actualmente predominan las compras online. Esto ha ocasionado numerosas estafas, los investigadores han precedido una estimación

de ocho millones de ataques diarios a través de las plataformas digitales (Lorenzo, 2021) . Sin embargo cuando pensamos en compras fraudulentas mediante los medios digitales nos viene a la cabeza que el producto que nos ofrecen realmente o no existe o es totalmente diferente pero, ¿Y si el fraude está en el comprador? Por ello me gustaría hacer hincapié en una técnica que cada vez es más habitual sobretodo en jóvenes en internet consistente en videos tutoriales para hacer compras fraudulentas. Estos recomiendan métodos como ocultar datos de conexión o falsificar los datos bancarios para así obtener el producto sin ningún tipo de desembolso (Familias, 2016).

VII. LA RESPONSIBILIDAD DE LOS PRESTADORES DE SERVICIOS EN LA RED

Los prestadores de servicios son aquellas personas, físicas y jurídicas, que ofrecen un servicio de información a la sociedad, es decir, servicio de plataformas o páginas en la web que actúan como intermediarios (De la Rosa Cruz, 2022).

Dicha responsabilidad se encuentra regulada en la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico[31].

Es un tema confuso ya que concurren diversos derechos de relevancia constitucional. Por un lado, encontramos el derecho del honor, a la intimidad y a la propia imagen y, por otro lado, las libertades de expresión y comunicación en internet. La controversia se fundamenta en la responsabilidad de los intermediarios por los contenidos publicados[32] por los usuarios, considerando si es necesario imponerles una sanción por ello o eximirles de responsabilidad (Barrero Ortega, 2021).

[31] Debemos destacar La Sección 230 de la Ley de Telecomunicaciones de USA la cual es el origen de la regulación actual. Dicha ley establece que: *"ningún proveedor o usuario de un servicio informático interactivo será tratado como el editor o hablante de cualquier información proporcionada por otro proveedor de contenido de información".*

[32] En el artículo 15 de la Directiva 97/66/CE se establece la prohición de los Estados Miembros de vigilar o interceptar dichos contenidos salvo que tengan la autorización pertinente.

La exención de responsabilidad se apoya en que el prestador de servicios no ha sido partidario ni de la creación ni de la difusión de contenidos ilícitos o perjudiciales.

Debemos resaltar así mismo que, es muy arduo controlar todo aquello que circula en sus redes debido al volumen de datos que se almacenan en las mismas. La Directiva sobre Comercio Electrónico ha fijado un sistema de exenciones en una serie de servicios muy precisos: los servicios de mera trasmisión, de provisión de acceso a la red, la actividad de almacenamiento temporal en *caching* y el servicio de alojamiento de datos o *hosting* (Peguera Poch, 2003).

Así mismo me gustaría destacar la sentencia del Juzgado de lo Mercantil nº 7 de Madrid, núm. 289/2010 de 20 de septiembre la cual fue el primer caso en el que una compañía de internet hacia frente a una demanda por una transgresión del derecho de propiedad intelectual. En esta sentencia las partes involucradas en el conflicto son "Telecinco", la cadena televisiva con numerosa audiencia diaria, y "YouTube", una de las plataformas digitales con mayor utilización tanto por jóvenes como por adultos.

Fue Telecinco quien tomó la decisión de presentar una demanda contra la plataforma acusándole de una vulneración en su derecho de propiedad intelectual por la divulgación de grabaciones audiovisuales pertenecientes a la otra parte sin consentimiento alguno.

La decisión del Tribunal Supremo radicaba en optar por hacer responsable, o no, a YouTube por la publicación de dicho contenido digital. La principal alegación que se utilizo fue que la plataforma ofrecía un espacio libre para que los usuarios hagan públicos sus videos pero que el control que la misma realizaba sobre estos no era exhaustivo. Por ello, el Tribunal Supremo decidió aplicar la exención de responsabilidad que explicaremos posteriormente (STC 289/2010).

Esta sentencia es muy relevante y, por ello he querido mencionarla como introducción al tema a tratar, porque a raíz de la demanda presentada se ha instituido un sistema para detectar, por parte de terceros, las posibles transgresiones que se cometan contra su derecho de propiedad intelectual demostrando de tal manera lo crucial que resulta la

colaboración entre los titulares de los derechos afectados y los intermediarios a la hora de desplegar actos en la web.

7.1 El encaje de las exenciones en el sistema general

En relación al régimen de responsabilidad de los prestadores de servicios, la LSSICE[33] afirma que están sujetos a una responsabilidad tanto civil como administrativa y penal, salvo la excepción que se encuentra expresada en el artículo 17 LSSICE y que involucra a los prestadores de servicios de la sociedad de la información que no posean un conocimiento real de la ilicitud de la acción cometida o el menoscabo que sobrelleva para terceros o para alguno de sus derechos. En el segundo apartado de dicho artículo se incluyen en la excepción y por lo tanto no tendrán responsabilidad alguna aquellos profesionales que, teniendo la certeza de la anticonstitucionalidad del hecho, traten de eludirlo o anularlo de manera eficiente.

Como hemos mencionado previamente, la directiva establece una serie de casos en los que no existe responsabilidad de los prestadores.

Los servicios de "mera trasmisión" que se encuentran regulados en el artículo 12 de la Directiva 2000/31/CE en el que se excluye la responsabilidad siempre y cuando el prestador de servicios no haya originado la trasmisión, no haya seleccionado al destinatario de la misma ni haya modificado los datos trasmitidos. Hace cuatro años el Caso C-484/14 cuestionó esta inmunidad de responsabilidad cuando se realizó una copia ilícita de una obra musical y consiguientemente, fue proporcionada a los usuarios de una página web con acceso no cifrado. Sr. McFadden, el prestador de dicho servicio, se escudó en la Directiva para formular su defensa negando así cualquier tipo de responsabilidad del mismo (Poysky & Torres, 2014).

En cuanto a las actividades conocidas como "Hosting" y "Caching", las exenciones instituidas son básicamente subjetivas. Estas varían en función de los requisitos de diligencia que le son exigidos al prestador de servicios. Si este ha cumplido con los

[33] LSSI-CE es la abreviatura de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico. Esta ley se encarga de regular las actividades de carácter económico que se desarrollan en Internet.

deberes que le son propios por su condición, no se le podrá acarrear culpa, es decir, se debe analizar minuciosamente cuál es el nivel de diligencia que se pide a estos profesionales[34].

7.3 Las "Cookies"

Las cookies son un medio utilizado por los prestadores de servicios en la red que les permiten almacenar y recuperar información o datos de navegación de los usuarios. Son una herramienta imprescindible que mejora nuestra navegación en la web, ya que han sido creadas con el objetivo de identificar a los internautas, recordar sus preferencias y ofrecerles un contenido acorde con sus intereses (Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital).

El artículo 22.2 de la Ley 34/2022, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) establece varias cuestiones (Uplalaunion, 2022).

La primera de ellas es que los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en los equipos terminales de los destinatarios, con la condición de que estos hayan dado su consentimiento después de haberles facilitado la información completa y clara sobre su utilización, en concreto, sobre los fines del tratamiento de los datos, acorde a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter Personal.

Así mismo cuando sea técnicamente posible y eficaz, el consentimiento para aceptar el tratamiento de datos podrá facilitarse mediante el uso de diversos parámetros en el navegador o de otras aplicaciones, siempre que aquél tenga la obligación de su configuración durante su instalación o durante cualquier actualización.

[34] El artículo 15.1 de la Directa: *"los Estados Miembros no pueden imponer a los intermediarios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14".* (Peguera Poch, uoc, 2003)

VIII. EL DERECHO AL OLVIDO Y EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

Derecho al Olvido:

"Internet nunca olvida" (Mda, 2018).
Como dice Álvarez Caro[35]: *"podría definirse como el derecho a equivocarse o a que una equivocación pasada no marque o determine la vida de un individuo"*.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo que entró en vigor el 25 de mayo de 2018, introduce nuevos elementos como el derecho al olvido. La posibilidad de borrar o bloquear información personal que se encuentre en internet ya sea porque es perjudicial para nosotros o porque vulnera alguno de nuestros derechos fundamentales es conocido como el derecho de supresión o el derecho al olvido. Según la AEPD: «*El derecho al olvido hace referencia al derecho que tiene el ciudadano a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa*» (Nando, 2016).

Frecuentemente el Derecho de supresión y el derecho al olvido son utilizados como sinónimos, pero, no obstante, dichos derechos son complementarios, no idénticos. El derecho de supresión se encarga de la eliminación de los datos e información de los individuos y el derecho al olvido trata de impedir la divulgación (Conceptos Jurídicos, 2021).
El derecho al olvido se encuentra recogido tanto en el Reglamento Europeo de Protección de Datos (artículo 17) como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (artículos 93 y 94).

A través del art. 93 LPDPGDD se expresa que todos los individuos poseen un derecho consistente en que todas las plataformas digitales deberán suprimir o eliminar todos aquellos datos que, debido al transcurso del tiempo, ya no se correspondan con los

[35] Autor del libro Derecho al olvido en internet: *el nuevo paradigma de la privacidad en la era digital*.

mismos o que sean completamente inadecuados, inexactos y que, por esta razón, les cause un detrimento tanto en su vida personal como profesional.

También encontramos una excepción en el segundo apartado de este articulo y es que este derecho al que todos tenemos acceso no supondrá un obstáculo para aquellos que indaguen en la web utilizando otros criterios que no sean la utilización del nombre de la persona que ha ejercido el derecho pero que, tengan una notoria relación con ella y eso les conduzca a dichos datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

Podemos encontrar diversos supuestos en los que el derecho al olvido puede ser ejercitado: cuando la finalidad principal de dicha información ya no es necesaria; si el derecho de oposición es ejercitado; si los datos son recogidos de manera ilegítima y sin ningún tipo de consentimiento o porque así lo establece el Derecho de la Unión Europea.

Así mismo, todo derecho tiene sus límites establecidos para que no concurra un abuso de este y entre los que nos encontramos los casos de interés público; el ejercicio del derecho a la libertad de expresión o para el ejercicio de otros derechos. Será necesaria la presentación de una solicitud por parte del titular para poder ejercitarlo, en la cual se estimará la misma o, por el contrario, será denegada.

Me gustaría hacer hincapié en el derecho al olvido en el ámbito de las redes sociales, recogido en la LOPDGDD. En las famosas plataformas como Facebook, Twitter o Instagram podemos configurar nuestra privacidad y deberemos informar a la red social de cualquier violación de las normas establecidas en las mismas que se produzca. Una vez comunicado el problema, las redes sociales estudiarán el caso y llevarán a cabo la eliminación de dicha información o perfil (Ayuda Ley Protección Datos, 2021).

Debemos destacar la sentencia de 15 de Octubre de 2015 dictada por el Tribunal Supremo que marcó límites, tanto en el derecho a la información como en el Derecho al olvido. En

ella está involucrado Mario Costeja[36], conocido como "el español todopoderoso que venció a Google" (2014).

Este abogado aparecía como dueño de una propiedad que había sido sacada a subasta debido a un impago de deudas, sin embargo, una vez saldadas e incluso habiéndose divorciado, Google le seguía calificando como moroso y casado. Tras una intensa lucha, consiguió que en el año 2010 la Agencia De Protección de Datos le diese la razón y solicitase al buscador la supresión de dichos datos personales (Romero, 2014).

Actualmente, gran parte de las empresas existentes en el mercado digital tienen un ferviente interés en la captación de un público infantil y juvenil ya que, son el colectivo que más tiempo dedica a la navegación en la web. Por esta razón, el Reglamento de Protección de Datos en la Unión Europea ha prestado y ha hecho gran hincapié en el Derecho al Olvido y el correspondiente trato de la información por la que los menores pueden quedar afectados protegiendo así, su identidad digital (Martínez, 2017). Debemos destacar que estas garantías que el ordenamiento ofrece deben fundamentarse en exhaustas políticas de prevención y concienciación ya que no hay mejor olvido que lo que nunca llegó a suceder y también que, a pesar de que la regulación vigente española está tratando de concretar y ser ambiciosa con este tema, es fundamental la cooperación y el papel que abarcan las familias y los educadores de los menores con la ley.

Este nuevo derecho será de notoria relevancia a partir de ahora ya que se trata de un medio de protección mayor de los internautas haciendo que, la "memoria" usuario tenga la posibilidad de poder desaparecer poco a poco.

Derecho a la Autodeterminación Informativa:

El derecho a la Autodeterminación Informativa otorga la voluntad a los individuos para la exposición de sus datos personales en el momento y del modo que estimen adecuado.

[36] Abogado gallego que consiguió que, por primera vez, el TJUE, ejercitara el derecho al olvido en internet.

Hasta el momento ha sido una medida empleada para la restricción de la información. En otras palabras, es la capacidad para llevar a cabo tanto la difusión como la utilización de datos, controlando lo que puedan llegar a conocer el resto de la sociedad. Es la autoridad de una persona para decidir sobre sí mismo. Este derecho integra la parte subjetiva del derecho a la intimidad. (Grupo Atico 34, 2021).

Por lo tanto podemos afirmar que nos encontramos ante un derecho inherente a la persona, personalísimo y objeto de respeto general por toda la sociedad.

Me gustaría mencionar la sentencia del Tribunal Constitucional 53/1985, de 11 de abril la cual tiene una gran relevancia porque el TC manifiesta, en relación al respeto de los derechos fundamentales del individuo, que el Estado no puede adquirir una actitud pasiva ante ello sino que, tiene el deber de garantizarlos de una manera activa y positiva, especialmente si existe el mandato legal expreso[37] (BOE núm. 119, 18 de mayo).

Es importante también hacer hincapié en el término "Habeas Data" que según afirma la RAE es: *"acción constitucional que puede ejercer cualquier persona incluida en un registro de datos para acceder al mismo y recabar la información que le afecte, así como para solicitar su eliminación o corrección si tal información fuera falsa o estuviera desactualizada".*

La importancia de este derecho radica en que el uso ilegítimo y el acceso a información personal atañen al derecho a la intimidad y de esta manera, a través de este medio, podemos preservar nuestra identidad, nuestra dignidad y nuestra libertad.

IX. CONCLUSIONES

Primera: La irrupción de Internet en nuestra sociedad y los avances en el desarrollo de las tecnologías se encuentran en continua aceleración día a día y eso provoca que, en numerosas ocasiones, nuestro ordenamiento jurídico no se encuentre lo suficientemente

[37] Recogido en el art. 18.4 de la Constitución Española.

capacitado para ajustarse a ellos quedando, los individuos desprotegidos. Especialmente la afectación inherente en los menores de edad, principales usuarios de la web que por razones de desconocimiento y falta de madurez no son conscientes de los riesgos que supone la publicación de contenido sin cautela.

Segunda: en la actualidad, las redes sociales son una gran herramienta capaz de incrementar tanto las sinergias y beneficios tanto individuales como colectivos de las individuos proporcionando innumerables posibilidades de estos. Sin embargo, estas plataformas pueden, de la misma manera, causar graves perjuicios tanto personal como profesionalmente en la vida privada de las personas por ello, la normativa y legislación vigente debe anticiparse al crecimiento y desarrollo de las redes sociales para poder evitar las situaciones perjudiciales de los ciudadanos encaminándoles hacia un correcto autocontrol y una autodeterminación.

Tercera: la privacidad en internet es un debate vigente y uno de los objetivos primordiales de nuestro ordenamiento jurídico. Esta preocupación se agrava si hablamos de los menores de edad, un colectivo que no posee el suficiente conocimiento acerca de los peligros que esconde la web. No obstante, no debemos aislar a los jóvenes sino concienciarlos y protegerlos sin vulnerar su libertad e intimidad.

Cuarta: la normativa en materia de protección de datos nos ofrece innumerables posibilidades para tener un control eficaz en relación a nuestra información publicada en las plataformas digitales, tratando de adaptarse a cada circunstancia y otorgando un trato diferenciado a los menores de edad.

Quinta: la evolución de las tecnologías ha creado nuevas formas delictivas a través de la web que afectan, especialmente a los jóvenes y a los adolescentes. La figura de los padres es imprescindible para evitar estos peligros pero, deben actuar con cautela y precaución respetando lo establecido en la ley ya que en numerosas ocasiones deberán tener el consentimiento expreso de su propio hijo y deberán velar por el interés superior del mismo.

Sexta: el derecho al olvido y el derecho a la autodeterminación informática son, ambos, inherentes a la persona y su importancia radica en que, gracias a ellos, podemos garantizar y proteger nuestra propia esfera personal frente a terceros.

Reflexión final: con el paso de los años, la tecnología ha evolucionado de una manera inimaginable tratando de satisfacer nuestras necesidades de la forma más sencilla posible.

Hoy en día somos incapaces de desarrollar nuestra rutina sin ella por ello, es imprescindible, debido a la cantidad de horas que pasamos delante de una pantalla, protegernos y tomar las medidas necesarias para privarnos de las consecuencias perjudiciales que conllevan. Especialmente debemos salvaguardar a los menores de edad, un colectivo calificado como vulnerable, que carece tanto de autodeterminación como del conocimiento necesario sobre el mundo digital.

Las redes sociales les proporcionan numerosos beneficios como el desarrollo personal o el intercambio de opiniones entre ellos y es por esa razón por la que tenemos el deber de tomar premisa y encargarnos de que cuenten con los medios necesarios para lograr su total protección.

No tenemos que subestimar ni nuestra seguridad ni nuestra privacidad, aún queda mucho camino por recorrer y nuestra tarea es tratar de asegurarnos de que las redes sociales eleven sus estándares de seguridad para ser capaces de adaptarse a las exigencias que van integrando la normativa existente acerca de la privacidad y el control en la web especialmente con los menores de edad.

X. BIBLIOGRAFÍA

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 298, de 14 de diciembre de 1999, pp. 43088-43099. https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. *Boletín Oficial del Estado*, 281, de 23 de noviembre de 1995, pp. 33987 a 34058.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 294, 6 de diciembre de 2018, pp. 119788-119857. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado, 17, de 19 de enero de 2008, pp. 4103-4136. https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979

Recurso previo de inconstitucionalidad número 800/1983. Sentencia número 53/1985, de 11 de abril. *Boletín Oficial del Estado*, 119, de 18 de mayo de 1985, pp 10-25. https://www.boe.es/buscar/doc.php?id=BOE-T-1985-9096

(s.f.). Obtenida el 25/03/2022 de Gobierno de España. Ministerio de Asuntos Económicos y Transformación Digital : https://lssi.mineco.gob.es/la-ley/aspectos-basicos/Paginas/obligaciones-responsabilidades.aspx

Conceptos Jurídicos. (25 de junio de 2021). Obtenida el 25/03/2022 de Derecho al Olvido: concepto, regulación y procedimiento: https://www.conceptosjuridicos.com/derecho-al-olvido/

AARP. (6 de DICIEMBRE de 2021). Obtenida el 3/04/2022 de https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/redes-sociales.html

Alcón Acedo Penco, A. y. (Diciembre de 2016). *Scielo*. Obtenida el 14/05/2022 de revista chilena de derecho y tecnologia:

https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842016000200063

Ambrojo, J. (7 de septiembre de 2006). *EL PAÍS: el periódico global*. Obtenida el 07/05/2022 de El País: https://elpais.com/diario/2006/09/07/ciberpais/1157593222_850215.html

Anónimo. (marzo de 2009). *PantallasAmigas, colaborador activo en el estudio publicado por INTECO sobre "Menores y TICs"* -. Obtenida el 04/03/2022 de PantallasAmigas: https://www.pantallasamigas.net/pantallasamigas-colaborador-activo-en-el-estudio-publicado-por-inteco-sobre-menores-y-tics/

Anónimo. (28 de septiembre de 2019). Obtenida el 07/05/2022 de abc: https://www.abc.es/familia/padres-hijos/abci-grooming-peligro-redes-sociales-para-hijos-201909280137_noticia.html#:%7E:text=El%20grooming%20es%20el%20acoso%20y%20abuso%20sexual,confianza%20para%20luego%20involucrarle%20en%20una%20actividad%20sexual&ref=

Anónimo. (3 de junio de 2020). *Cómo prevenir el Sexting en Redes Sociales*. Obtenida el 06/05/2022 de CiberIntocables: https://ciberintocables.com/prevenir-sexting-redes-sociales/

Arjona, A. (7 de noviembre de 2021). *ESTAFAS INFORMÁTICAS*. Obtenida el 25/05/2022 de ARJONA ESTUDIO JURÍDICO: https://arjonaestudiojuridico.com/2021/09/27/estafas-informaticas/

Ayala, S. (2 de noviembre de 2018). *"EL PELIGRO DE LAS REDES SOCIALES" SEXTING Y GROOMING | Asociación Mexicana de Psicoterapia y Educación*. Obtenida el 25/05/2022 de Asociación Mexicana de Psicoterapia y Educación | Formación profesional en Psicología, Psicoterapia y Educación: https://www.psicoedu.org/el-peligro-de-las-redes-sociales-sexting-y-grooming/?v=55f82ff37b55

Ayuda Ley Protección Datos. (20 de julio de 2021). Obtenido de Derecho al olvido o de supresión : https://ayudaleyprotecciondatos.es/derecho-olvido-supresion/

Ayudaley. (s.f.). Obtenida el 16/05/2022 de Derechos ARCO. Nuevos ARCO-POL ¿Qué son y como ejercerlos?: https://ayudaleyprotecciondatos.es/derechos-arco/

Balderas Blanco, S. (5 de junio de 2015). *Internet: un espacio de difícil control sobre los menores de edad*. Obtenida el 05/04/2022 de https://elderecho.com/internet-un-espacio-de-dificil-control-sobre-los-menores-de-edad

Barrero Ortega, A. (31 de Diciembre de 2021). *Revista Española de Derecho Constitucional*. Obtenida el 07/05/2022 de Responsabilidad de los intermediarios de internet en el Derecho de la UE: https://recyt.fecyt.es/index.php/REDCons/article/view/92767/67573#:~:text=La%20Directiva%20sobre%20el%20comercio%20electr%C3%B3nico%20exime%20a%20los%20ISP,tengan%20%C2%ABconocimiento%20efectivo%C2%BB%20de%20la

Belcic, I. (5 de Febrero de 2020). *Avast Academy* . Obtenida el 06/05/2022 de https://www.avast.com/es-es/c-phishing#topic-2

Beloki, M. (4 de Octubre de 2021). *Datcon Norte*. Obtenida el 06/05/2022 de ¿Qué consentimiento necesitamos para el tratamiento de datos de menores?: https://www.datcon-norte.com/que-consentimiento-necesitamos-para-el-tratamiento-de-datos-de-menores/

Bienestar y protección infantil . (s.f.). Obtenida el 08/05/2022 de https://www.bienestaryproteccioninfantil.es/fuentes1.asp?sec=13&subs=13&cod=110&page

Borondo, S. (19 de agosto de 2021). *Los 10 mayores peligros para los adolescentes en las redes sociales (y cómo prevenirlos)*. Obtenida el 05/04/2022 de El Correo: https://www.elcorreo.com/tecnologia/redes-sociales/mayores-peligros-adolescentes-20210805123452-nt.html

Calvo Rodríguez, A. (Julio de 2018). *Trabajo Fin de Grado.* Obtenida el 06/05/2022 de La protección jurídica del menor en internet: https://gredos.usal.es/bitstream/handle/10366/139137/TG_CalvoRodriguez_Proteccion.pdf;jsessionid=A8BC26218E04A092614ECB03FC8F095B?sequence=1

Ciberbullying: ¿qué es y cómo lo prevenimos? (6 de agosto de 2018). Obtenida el 07/05/2022 de Ayuda en Acción: https://ayudaenaccion.org/blog/educacion/ciberbullying/

Consulting, E. (28 de Noviembre de 2012). *Eurovima*. Obtenida el 07/05/2022 de Redes Sociales I; Aspectos Normativos: https://eurovima.es/blog/redes-sociales-y-lopd/

Davara Fernández de Marcos, L. (2016). *Agencia Española de Protección de Datos*. Obtenida el 07/05/2022 de https://www.aepd.es/sites/default/files/2019-10/menores-en-internet.pdf

Davara Fernández de Marcos, L. (s.f.). Régimen jurídico de las redes sociales. *Vlex*, 205 .

De la Rosa Cruz, J. Á. (2022). Obtenida el 09/02/2022 de Responsabilidad de los prestadores de servicios en la LSSI: https://delarosacruz-abogado.com/responsabilidad-prestadores-servicios-lssi/

Del Águila, M. (26 de Noviembre de 2018). *GlobalSuite Solutions*. Obtenida el 04/04/2022 de https://www.globalsuitesolutions.com/es/nueva-lopd-consentimiento-menores/

Ehmke, R. (15 de febrero de 2022). *Cómo afecta el uso de las redes sociales a los adolescentes*. Obtenida el 06/05/2022 de Child Mind Institute: https://childmind.org/es/articulo/como-afecta-el-uso-de-las-redes-sociales-los-adolescentes/#%C2%BFqu%C3%A9-deber%C3%ADan-hacer-los-padres

Esténtor. (s.f.). Obtenida el 03/05/2022 de El derecho fundamental a la protección de datos: https://blog.estentor.es/derecho-fundamental-proteccion-datos#:~:text=La%20protecci%C3%B3n%20de%20datos%20es%20un%20dere

cho%20fundamental%2C,m%C3%A1s%20espec%C3%ADficas%20que%20la%20regulen%20y%20la%20ejecuten.

Familias. (27 de Septiembre de 2016). *is4k*. Obtenida el 06/05/2022 de https://www.is4k.es/blog/compras-fraudulentas-y-menores-cuando-el-fraude-esta-en-el-comprador

Ferrer, M. (20 de agosto de 2021). *Los riesgos de las redes sociales para los adolescentes que debes conocer*. Obtenida el 06/04/2022 de El Comercio: https://www.elcomercio.es/sociedad/riesgos-redes-sociales-adolescentes-jovenes-20210820182414-nt.html?ref=https%3A%2F%2Fwww.google.com%2F

Fuente Cobo, C. (s.f.). La Protección del Menor tras la Ley General de la Comunicación Audiovisual. *iCmedianet*, 20.

García, N. (13 de Septiembre de 2016). *Editorial Jurídica Sepin* . Obtenido de 06/05/2022 de ¿Pueden los padres violar realmente la intimidad de los menores?: https://blog.sepin.es/2016/09/intimidad-menores-control-parental/

Gersonvidal. (7 de enero de 2022). *Servilegal Abogados*. Obtenida el 09/05/2022 de Delito contra el honor, injuria y calumnia: https://www.gruposervilegal.com/delito-contra-el-honor-injuria-y-calumnia/#:%7E:text=Los%20delitos%20contra%20el%20honor%20son%20la%20injuria,Penal%2C%20que%20abarca%20del%20art%C3%ADculo%20205%20al%20216

Gil Antón, A. (2013a). *El ambito de internet, el fenomeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales*. Obtenida el 07/05/2022 de vLex: https://vlex.es/vid/internet-fenomeno-redes-fundamentales-481818454

Gil Antón, A. (2013b). La Privacidad del Menor en Internet. *Unir*, 75-78. Obtenido de file:///Users/alvarogonzalez/Downloads/Dialnet-LaPrivacidadDelMenorEnInternet-4764226.pdf

Gil Antón, A. M. (2013a). La Privacidad del Menor en Internet . *UNIR*, 64-75.

González, F. (11 de diciembre de 2021). *El riesgo de las redes sociales para la salud mental de los adolescentes*. Obtenida el 09/05/2022 de Batiburrillo - De todo un poco: https://www.batiburrillo.net/el-riesgo-de-las-redes-sociales-para-la-salud-mental-de-los-adolescentes/

Grooming, qué es, cómo detectarlo y prevenirlo. (1 de julio de 2019). Obtenida el 09/04/2022 de Save the Children: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Grooming, qué es, cómo detectarlo y prevenirlo. (7 de febrero de 2022). Obtenida el 09/04/2022de Save the Children: https://www.savethechildren.es/actualidad/grooming-que-es-como-detectarlo-y-prevenirlo

Grupo atico 34. (2021). Obtenida el 08/03/2022 de https://protecciondatos-lopd.com/empresas/redes-sociales-lopd/#:~:text=Entre%20las%20obligaciones%20impuestas%20por%20la%20ley%20de,protecci%C3%B3n%20de%20datos%20y%20la%20pol%C3%ADtica%20de%20privacidad.

Grupo Atico 34. (2021). Obtenida el 07/02/2022 de Autodeterminación informativa. Concepto y cómo ejercerla: https://protecciondatos-lopd.com/empresas/autodeterminacion-informativa/

Herce Ruiz, B. (2012a). Aspectos Jurídicos Sobre la Privacidad en las Redes Sociales. *Trabajo Fin de Máster*, 14.

Herce Ruiz, B. (2012b). Aspectos Jurídicos sobre la Privacidad en las Redes Sociales. 15.

Iberley . (22 de Julio de 2021). Obtenida el 09/03/2022 de El consentimiento en la Ley Orgánica 1/1982, de 5 de mayo (derecho al honor, intimidad, propia imagen): https://www.iberley.es/temas/consentimiento-1-1982-5-mayo-derecho-honor-intimidad-propia-imagen-65508

Iberley. (25 de Abril de 2017). Obtenida el 07/03/2022 de https://www.iberley.es/jurisprudencia/sentencia-civil-n-268-2017-ap-barcelona-sec-4-rec-693-2016-25-04-2017-47872667

Intef. (s.f.). *Intef* . Obtenida el 07/04/2022 de Seguridad del menor en Internet: https://intef.es/tecnologia-educativa/seguridad-del-menor-en-internet/

León, J. d. (s.f.). *Internet Segura*. Obtenida el 05/05/2022 de Las acciones de información, formación y sensibilización ante los riesgos de las nuevas tecnologías: https://www.educa.jcyl.es/ciberacoso/es/plan-prevencion-ciberacoso-navegacion-segura/fomento-buen-uso-medios-informaticos/acciones-informacion-formacion-sensibilizacion-riesgos-nuev

Llamas Bao, C. (2021). *Revista Jurídica de la Universidad de León*. Obtenida el 06/05/2022 de http://revpubli.unileon.es/ojs/index.php/juridica/article/view/7080

Lleida, J. R. (11 de Octubre de 2021). *La Vanguardia*. Obtenida el 07/05/2022 de https://www.lavanguardia.com/tecnologia/actualidad/20211011/7782012/fraude-internet.html

Lorenzo, j. a. (29 de Noviembre de 2021). *Redes Zone*. Obtenida el 06/04/2022 de https://www.redeszone.net/noticias/seguridad/compras-online-aumentan-ciberataques-estafas/

Mario Costeja, el español que venció al todopoderoso Google. (14 de mayo de 2014). Obtenida el 04/05/2022 de La Vanguardia: https://www.lavanguardia.com/tecnologia/internet/20140514/54407896513/mario-costeja-google.html

Martínez, R. (24 de Mayo de 2017). *Universitat de Valencia.* Obtenida el 09/05/2022 de El derecho al olvido de los menores.: https://www.uv.es/catedra-

microsoft/es/catedra-privacidad-transformacion-digital-microsoft-uv-1285992809525/GasetaRecerca.html?id=1286007057307

Mateo Bueno, F. (2014). *Mateo Bueno, abogado de familia.* Obtenida el 07/05/2022 de https://www.mateobuenoabogado.com/publicacion-de-fotos-de-menores-en-las-redes-sociales/

Mda, G. (30 de enero de 2018). *Internet nunca olvida: por qué la huella digital que dejamos en las redes nos traerá consecuencias*. Obtenida el 09/03/2022 de https://culturacolectiva.com/tecnologia/internet-nunca-olvida-huella-digital/

Nando. (17 de noviembre de 2016). *EL DERECHO AL OLVIDO Y GOOGLE*. Obtenida el 04/05/2022 de El Abogado Digital: https://www.elabogadodigital.com/el-derecho-al-olvido-y-google/

Nogueira, J. (24 de Abril de 2020). *Sistemius* . Obtenida el 04/05/2022 de Responsabilidad de los prestadores de la sociedad de la información: https://www.sistemius.com/prestadores-de-la-sociedad-de-la-informacion/

Owaida, A. (3 de junio de 2021). *we live security*. Obtenida el 04/03/2022 de https://www.welivesecurity.com/la-es/2021/06/03/5-estafas-comunes-dirigidas-a-los-adolescentes-y-como-protegerse/

Peguera Poch, M. (Enero de 2003). *UOC*. Obtenida el 05/03/2022 de IN3: https://www.uoc.edu/in3/dt/20080/index.html

Poysky, A., & Torres, A. (3 de Diciembre de 2014). *uaipit*. Obtenida el 04/04/2022 de https://www.uaipit.com/es/noticias/3274/caso-c-484/14-cuestiona-la-responsabilidad-de-una-mera-transmision

Rius, M. (29 de junio de 2012). *Mi otro yo de las redes sociales*. Obtenida el 04/04/2022 de La Vanguardia: https://www.lavanguardia.com/estilos-de-vida/20120622/54314745034/mi-otro-yo-de-las-redes-sociales.html

Roig Rosselló, M. (15 de octubre de 2020). *EL DELITO DE ACOSO O STALKING (art. 172 ter Código Penal)*. Obtenidoa el 04/03/2022 de Roig & Roig Asesores | Economistas, Abogados y Auditores en Lleida: https://roigiroig.com/es/delito-stalking-acoso/

Rojas, Y. (2017). Obtenida el 04/04/2022 de https://adabogados.net/sexting-el-delito-en-las-redes-sociales/#:%7E:text=Los%20supuestos%20t%C3%ADpicos%20de%20sexting%20son%20el%20reenv%C3%ADo,de%20encuentros%20ciber-sexuales%20con%20la%20v%C3%ADctima%20por%20Skype

Rojas, Y. (2017). *Área Digital Abogados*. Obtenida el 08/05/2022 de Sexting: el delito en las redes sociales: https://adabogados.net/sexting-el-delito-en-las-redes-sociales/#:%7E:text=Los%20supuestos%20t%C3%ADpicos%20de%20sexting%20son%20el%20reenv%C3%ADo,de%20encuentros%20ciber-sexuales%20con%20la%20v%C3%ADctima%20por%20Skype

Romero, P. (13 de mayo de 2014). *Mario Costeja frente a Google: ' Yo defendí la libertad de expresión recibiendo hostias de los grises'*. Obtenida el 08/05/2022 de ELMUNDO: https://www.elmundo.es/tecnologia/2014/05/12/53709f5ce2704e902e8b4573.html

Sesma Goñi, T. (16 de Enero de 2018). Trabajo de Fin de Grado. *Protección de datos de carácter personal*. Pamplona.

Unicef. (11 de Diciembre de 2017). *Unicef: para cada infancia*. Obtenida el 06/05/2022 de https://www.unicef.org/es/comunicados-prensa/unicef-pide-proteger-los-ni%C3%B1os-en-el-mundo-digital-al-tiempo-que-se-mejora-el

Uplalaunion. (2022). Obtenida el 06/05/2022 de https://uplalaunion.org/politica-de-cookies/

Uplalaunion. (2022). *Uplalaunion*. Obtenida el 06/05/2022 de https://uplalaunion.org/politica-de-cookies/